Secure and Lightweight Authentication Protocols For Devices In Internet of Things

Kanthi Sree Addanki

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Secure and Lightweight Authentication Protocols For Devices In Internet of Things

Thesis submitted in partial fulfillment

of the requirements of the degree of

Masters of Technology

in

Computer Science and Engineering

by

Kanthi Sree Addanki

(Roll Number: 214CS2143)

based on research carried out

under the supervision of

Prof. Bibhudatta Sahoo

May, 2016

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Prof. Bibhudatta Sahoo
Assistant Professor

May 20, 2016

Supervisor's Certificate

This is to certify that the work presented in the dissertation entitled *Secure and Lightweight Authentication Protocols For Devices In Internet of Things* submitted by *Kanthi Sree Addanki*, Roll Number 214CS2143, is a record of original research carried out by her under my supervision and guidance in partial fulfilment of the requirements of the degree of *Masters of Technology* in *Department of Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

_____
Bibhudatta Sahoo

Dedication

I here by dedicate my thesis to my family who have been so supportive throughout my career.

Signature

Declaration of Originality

I, *Kanthi Sree Addanki*, Roll Number *214CS2143* hereby declare that this dissertation entitled *Secure and Lightweight Authentication Protocols For Devices In Internet of Things* presents my original work carried out as a postgraduate student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

May 20, 2016
NIT Rourkela

Kanthi Sree Addanki

Acknowledgment

There have been many ups and downs throughout the course of my research. Yet, the journey was successful because of the wonderful people who have been there to offer support throughout my research.

First and foremost, I would like to express my earnest gratitude towards my advisor Prof. Bibhudatta Sahoo for his incredible support in my M.tech research. I am truly grateful for his patience, motivation, enthusiasm, and immense knowledge which has been a driving force in my research. His guidance has helped me in all aspects of research and in writing this thesis. To sum up, I could not have imagined having a better advisor for my research work and as a mentor in my life.

I would also like to express an immense gratitude to the entire faculty of the Department of Computer Science and Engineering for providing me with an outstanding level of help and academic facilities.

I would deeply thank all the technical staff as well as the administrative staff of the college who have been kind enough to advise and help me in my journey.

Finally, I would like to thank all my fellow students and my best friends for their tremendous help throughout my research. I owe my endless gratitude to everyone who have made this work possible and made this M.tech experience one that I would cherish forever. I am forever indebted to my entire family for their unconditional love and encouragement throughout my life.

May 20, 2016
NIT Rourkela

Kanthi Sree Addanki
Roll Number: 214CS2143

Abstract

The Internet of Things (IoT) is becoming an intriguing trend worldwide as it allows any device to create and participate in a highly immersive and connected environment that integrates physical, digital and social aspects of the users and reacts according to the user requirements. The success of an IoT application depends on how well it fulfills certain design considerations like reliability, quality of service, security,scalability of the applications, among which security issues gain more importance in real world because the exposure of vulnerabilities in IoT applications can have serious consequences and it is important to set up improved mechanisms for assuring security. The perpetual growth in the number of devices tends to create more vulnerabilities if these devices are not authenticated before the device communicates critical data with the servers. However, designing a security mechanism for IoT is a challenging task due to the resource-constrained nature of the underlying sensor elements in the network.

In this thesis, a need for authentication of the devices in perception layer of the IoT architecture is discussed. A centralized network model is considered where the devices in the perception layer are mutually authenticated with the gateway of the system using their credentials. A secure and lightweight mutual authentication mechanism using symmetric key negotiation using a variant of Elliptic Curve Cryptography(ECC), Elliptic Curve Diffie-Hellman(ECDH) is proposed in the device registration phase of the protocol to protect the credentials of the devices with lesser key size itself and also to minimize the computation cost of devices. At the end of the authentication, key agreement based on the symmetric key cryptography is established between the sensor devices and the gateway so that further the devices can carry out data collection and acquisition tasks securely and efficiently without any attacks from adversary. Further, Elliptic Curve Integrated Encryption Scheme (ECIES) method is used to avoid the possibility of man-in-the-middle attack in the initial phase of the protocol and the results are recorded. The performance evaluation with the existing schemes based on the execution time and computation cost at the device has been performed after the protocol is simulated in the Cooja simulator under Contiki OS environment. The comparison results show that the proposed system provides low computation cost and satisfies the necessary security requirements.

***Keywords*: *Internet of Things*; *Security*; *Lightweight Authentication*; *Elliptic Curve Cryptography*; *ECDH*; *ECIES*.**

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Internet of Things concept is growing quite popular which is all about control and automation, reducing expenses, efficient communication of the things which are connected to internet. The things in this context refer to the heterogeneous power constrained devices with inbuilt RFID's, sensors, actuators, or any smart communication interfaces[1]. A device is a part of a thing and it can be a sensor or actuator or it can be a tag. The tasks of the things include collecting contextual information from devices and send the processed information to the other devices. Furthermore, the thing can pass actions to actuators[2]. A thing can not only be a car or a watch but can also be abstracted to a home or a city depending on the use case scenario.These things with unique IP address are able to communicate with each other to perform certain tasks with minimal human involvement to lessen the burden of the users.

However, these IoT devices mostly follow wireless communication which raises curtain for various security challenges which are related to wireless sensor networks[2, 3]. The problem of node authentication in the network is always a concern in wireless sensor networks. In case of IoT, whenever a device initiates the communication, be it data collection, data aggregation, there is a possibility for the intrusion of attackers in the form of eavesdropping or impersonating the device. This will not only provide the attacker, access to the critical data of the communication but also the ability to modify the settings of the devices. For example, the lack of authentication in the body area networks used in health care applications of IoT, results in the intrusion of adversaries in the form of invalid devices which can be capable of issuing false instructions to the patient's devices causing severe damage to their health[4]. Mostly these devices are susceptible to different security attacks like impersonation, replay attacks which brings up the imperative need for a security mechanism which checks the authenticity of the devices before the data collection and data acquisition tasks[5, 6]. Besides, these IoT devices possess limited memory and processing power[7], which causes draining of resources which brings the necessity for these secure cryptographic protocols to be lightweight protocols as well in order to reduce the computation overhead and prolong their lifetime[8].

There are different authentication models for different network environments. In this thesis, the proposed device authentication mechanisms are lightweight in nature which achieves mutual authentication as well as key agreement using symmetric key negotiation and asymmetric cryptography. These protocols are devised for the authentication between IoT devices and the gateway of the network.

1.1.1 Architecture of IoT

There are various architectures for Internet of Things proposed by the researchers such as 3-layered,4-layered,5-layered architectures. However, all these different architectures essentially define the three functionalities of IoT like perception,transmission and processing [9].

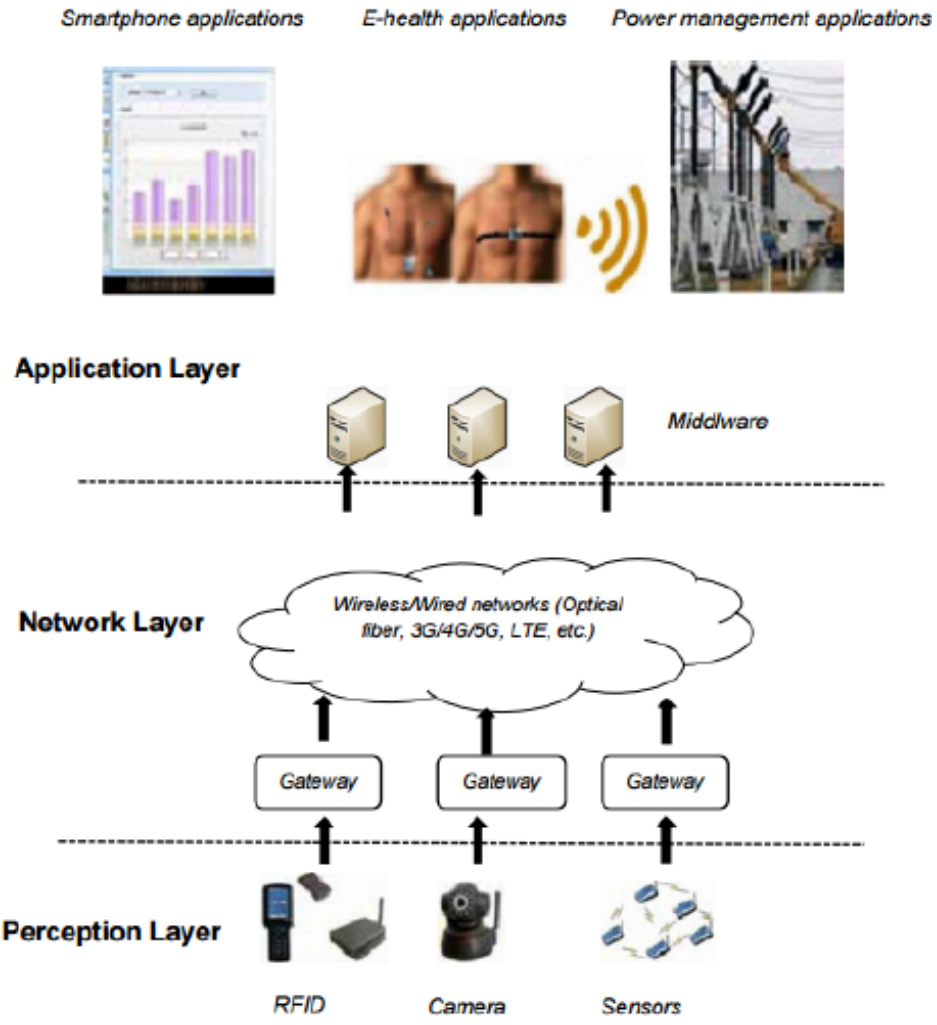

Figure 1.1: 3-layered Architecture of Internet of Things

Perception Layer

Perception Layer of IoT is the layer which describes about the heterogenous things of IoT such as sensors, RFID's, actuators, mobile phones. The main function of this layer is to acquire, collect and process the data from perception devices such as RFID's, temperature and humidity sensors, wearables and also control the actuators such as heater, fan[10]. This layer is responsible for transforming the information collected from sensors into digital signals to forward to the upper network layer.

Types of Things "Things" in the Internet of Things can be classified into following categories[11]:

1. **Tagging things:** The objects like RFID's are categorized as tagging things.
2. **Sensing things:** The objects like sensors present in wireless sensor networks are categorized as sensing things.
3. **Shrink things:** The objects like nano materials, nano processors of nano technology can be categorized as shrink things.

Sensing things are the category of devices that are being used in the following sections.

Network Layer

The main function of network layer is to transmit and process the information collected by sensors of the perception layer[9]. The network layer includes communication network technologies, information and intelligent processing center. This layer will send the digital signals received from the perception layer to the upper layers using one among the various communication networks such as WLAN, mobile adhoc network etc. All these components of the network layer are meant to be robust enough to meet the requirements like addressing, resource management, network integration.

Application Layer

The Application Layer acts like an interface between other layers and the users[12]. The main task of this layer is to integrate the lower layer functionalities and create a practical platform for all types of scenarios, such as the environmental monitoring, intelligent transportation, medical and health monitoring, home automation. This layer provides the required services to the customers. For example, the queries like measurements of the temperature, humidity parameters are sent back to the customer who needs that data. The significance of this layer is to able to provide exceptional quality services as per the customer queries. This layer includes numerous varieties of applications like smart buildings, smart cities and homes etc.[13].

1.1.2 Key Principles and Elements of IoT

The key point of IoT can be summarized as follows[14] :

- Four important underlying technology fields that lay foundation for IoT are the sensors,addressing,networks,distributed identification
- Three types of communication such as thing to person, person to person, thing to thing are possible.
- The large quantities of data accumulated from the heterogeneous sdeviceswhich is processed further will be increasing in volume day by day.
- Most of the communications will occur automatically, devices will have the ability to decide to exchange data within their environment and more likely without the actual user's knowledge.
- There exists context awareness among the devices and their heterogeneity provides quite large number of functionalities in different domains.

The following are the key elements of the IoT Technology:

IoT is a complete technology ensemble which includes various categories like the device technology to sense the real world data, data transfer technology to commute this data to different devices spread across the confined area, the intelligent process technology to merge and process the loads of data into real world applications.

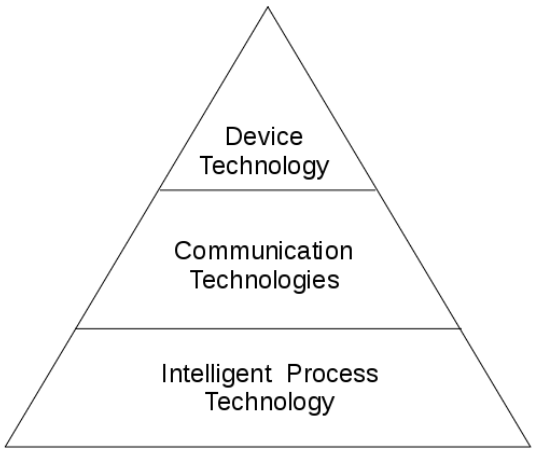

Figure 1.2: Technologies of Internet of Things

1. Device Technology:

The first technology ruling the IoT world is the sensor and actuator technology. This part acts as the enabler for gathering of data by various means such as sensors,tags. RFID is one

among the wide range of available device technologies. They are capable of detecting the movements of fast-moving objects using the embedded tags.

Besides this, another driving force for data collection is the sensor technology which are inserted into the devices to help in the transformation of the physical world objects into the smart objects. The sensing unit and the power unit present in the sensor device are the building blocks of the smart object. They help to find the signals around the devices and act accordingly. The actuator unit is incorporated in the same unit of sensor which is responsible for the transformation of energy into sensor movements.

2. Communication Technology:

In order to enable the successful communication among the device technologies, there is always a imperative requirement for the communication protocols. As far as the types of technologies for communication are concerned, there are two varieties such as the wired and wireless. The wired

Application Layer	CoAP,MQTT, XMPP
Network/ Communication Layer	IPv6,RPL, 6LoWPAN
Perception Layer	IEEE 802.15.4

Figure 1.3: Communication Protocols Stack of Internet of Things

In case of IoT, the most crucial technology used for communication among the sensing devices are the wireless protocols. They act as a bridge between the device technology and the processing aspect of IoT. This wireless sensor networks impart the necessary perception ability to IoT. The following figure shows the communication stack of IoT protocols.

3. Processing Technology:

The enormous loads of data from the perception layer tags and sensor devices is usually very difficult to process with the traditional technologies. Hence an improved intelligent processing technology such as a data manager collaborated with cloud is used for this purpose. This technology automates the process of dividing the loads of data into different chunks for making the processing and storage steps easier. The distributed nature of the cloud acts as an ensemble of many programs to handle the enormous data communication.

1.1.3 Applications

IoT is a vast area growing in every possible direction with a vast variety of applications in diverse domains. The IoT applications can be segregated into different categories based on several factors like type of network availability, scalability, heterogeneity of the things, degree of automation and impact[15]. We can divide the wide range of applications into the following groups:

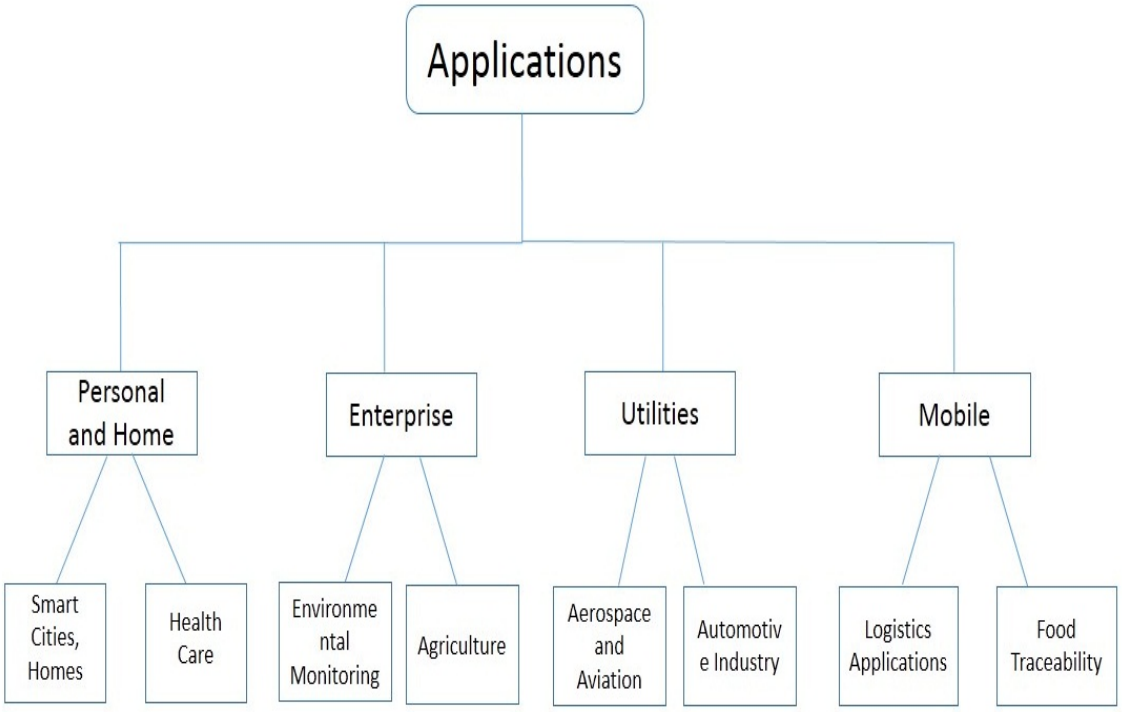

Figure 1.4: Applications of Internet of Things

Personal and home

In personal domain category, information from the perception layer is collected and this data is used only by the users who directly own the network. Ubiquitous healthcare[16] is yet another platform which is depicts the essence of IoT with the help of body area sensors. The day-to-day devices such as smartphone is a perfect media to control the communication with the help of other interfaces such as bluetooth to connect the sensors to find the measurements of various parameters.

The automation employed in home appliances such as fridge, washing machine delivers a better power management and their efficiency.

Enterprise

The enterprise applications are supposed to be defined as IoT enforced within work environment. The external information received by the network is accessed by the sole

owners of the enterprises. Once the data is collected, the broadcast of this data into the real world is performed by them. This is usually observed in case of agriculture and also to keep the count of tenants in the buildings in case of environmental monitoring.

The significant area of IoT applications is the Smart Environment IoT[17]. The applications of urban environment can gain benefits from the creation of a smart city with the usage of WSN. They include areas such as health, transport and mobility.

Utilities

Unlike other application domains, the data obtained from the outside world is used for improvement of services. The users who avail this facility include the smart electricity supply firms who strive to improve the trade-off between cost and profit. In order to manage the vital utilities and resources efficiently, an extensive group of networks is used to create their networks. Smart grid, metering is another wide domain of IoT which has popularity all over the world[18]. This works based on the information collected at the city and it is used for reaching the specified quality of service with the load balancing.

One of the popular utilities of IoT is monitoring the network of water and its quality. Many sensors are integrated into the localities in order to calculate the required parameters to ensure more quality in supply is achieved by eliminating the problems of spoiling drinking water, wastage disposal. The similar network is followed in agriculture utility as well to make decisions about soil quality and related parameters[15].

Mobile

Smart logistics and transportation are another potential application in this domain. The pollution created by the whole urban traffic has become a major concern in most of the cities. To avoid this condition, the traffic management should be transformed dynamically. For this, IoT can be used to design online traffic monitoring using wider WSNs. Based on the captured information, only relevant data is broadcasted to the travelers.

Yet another widely used application is the bluetooth which is mostly used in numerous products like hand sets, smart phones etc. The sensors used in bluetooth are able to read the signals emitted by the devices in close proximity. However, there prevail huge privacy issues related to this usage. Digital forgetting is one evolving area to be studied where the main concern is privacy.[17]

The major share of the mobile domain is occupied by the logistics category. The activities involved in this domain are checking the levels of efficiency in transport along with its planning. This is mainly achieved by using an IoT network to large extent.[19].

1.2 Research Challenges in IoT

Despite the enormous applications, IoT has certain challenging areas which needed to be focused. The research challenges of IoT can be summarized as[20–22]:

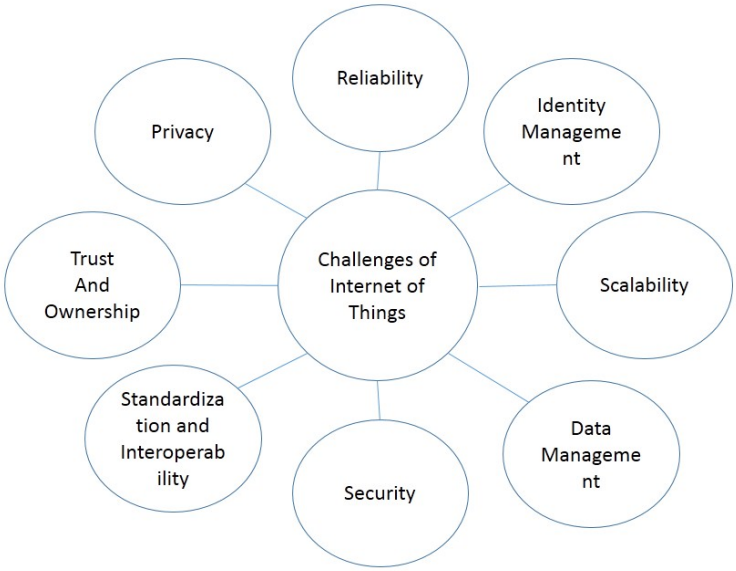

Figure 1.5: Challenges of Internet of Things

Privacy

The soaring number of devices in the IoT technology is the reason for privacy issues to become more prevalent. In order to improve the usage and levels of comfort of the users of IoT, it is vital not only to secure the data but also to solve the ownership issues regarding the data privacy.

Thus, whenever the data is collected, it is the main task to assign the ownership very clearly. By doing this, it is ensured that a barrier has been set on the permissions to use the data that is being shared which can be managed only by the owner. All the objects are capable of having their own privacy rules which are used by each other while communicating over the internet. [23].

Security

It is very essential for the IoT technology to provide security as per the demand such as Intranet wise, data wise, software and hardware wise as well as for the physical aspects.[21]. Communication in Internet is typically secured by carrying ot encryption over the channel. This is the possible way to promise the security of the data in IoT. However, the vey low resource capacity of IoT doesn't completely have the facility to support the complex operations. Hene, focus is put on reducing the complex nature of this encryption so that they are able to provide better efficiency and key management. [2, 24]

The current resource-constrained nature of the IoT resembles the sensors in WSNs in terms of communication, the available wireless channels, the ability to process the huge data, attack prone features. All these elements make it more difficult to enforce secure services for the things in IoT. The reasons behind these difficulties being the heterogeneity and the insecure environment where these devices have been deployed. Also, the global accessibility for these devices is provided using various protocols like RPL, CoAP over the wireless links in the communication.

Reliability

The degree of unreliability and uncertainty introduced in IoT environments following the real-world dynamics, makes such environments error prone. Enhancing the reliability of the devices and the data requires new strategies for managing them and providing ireliability patterns within IoT environments. Such strategies refer to methods for identifying reliability and reputation patterns for the things, the quality of information.Mechanisms are required that will enable the dynamic linkage between things and their attributes.

Trust and Ownership

The design of the infrastructure incorporated in the IoT helps to carry out communication between various hosts, end-to-end systems along with the intermediate parties. This raises the concern for the need of trust on both sides of communicating parties. In this case, this trust should be established not only between devices but also in the protocols being used by these entities. During this course, the factor of ownership also comes into picture which defines how one device is relying on another while performing the necessary commands and dedicated tasks. [21].

Scalability

There is every possibility in IoT to face the challenge of scalability. Because of the pace at which the growth of the IoT devices such as sensors etc is the cause for the growth in the accumulation of the data from them tremendously[21]. The ways to expand the IoT environment are by ensuring the lifetime of the devices, their security. Thus handling scalable issues hugely depends on the number of entities in the network and the information produced by them. [25].

Standardization and Interoperability

Any practical application of IoT is the combination of mainly different actors like things and users in the infrastructure. Accordingly, the responsibilities of these elements also vary depending on the type of application such as aggregation, collection etc. The main contribution of these actors towards IoT is how well they interact with each other. Thus the standards as well as the interactions play an eminent role to achieve the communication

goals of IoT.[25].

Identity Management

The process of integrating the zillions of objects into the IoT environment and the maintenance of the details of those devices is a tedious task. The way these things are provided with address requires the quality of uniqueness which is another task to be taken care of accordingly. There are several vital technologies like the smart cards, pins, tags etc. are considered as a means to address the devices in the IoT[7]. Hence, the task of providing identities has gained so much importance in most of the security frameworks in IoT. Because they help to find out the fraud activities in institutions, organizations. Thus, identity management ensures that these smart entities are who they claim to be in the IoT applications[26].

Data Management

The first problem that the developer of IoT needs to consider is the data extraction which can be regarded as the work on how to collect the data from the appliances and then to extract useful information from the collected data. Apparently,how data is extracted will have a strong effect in such environment, especially when the number of appliances are increased to a certain number. Different from the data extraction issues, the data representation is another important research topic because the common data representation may be contributory to information exchange between the IoT system and others, such as ontology and semantic web technologies[21].

1.3 Taxonomy of Security Concerns in IoT

Internet of Things platform is usually deployed using various communication and design technologies depends on the needs of the target application. The traditional security threats related to internet cannot be applied on the IoT. However, it is recommended to propose dedicated threat models for IoT applications. The degree of heterogeneity present in the IoT systems is one of the causes for the prevalence of numerous security threats in the target IoT applications.

Security in IoT system is classified as follows [4].

1. Data Security
2. System Security

1.3.1 Data Security

Sensor networks is a key part of IoT. All the existing IoT devices are most likely tiny and resource constrained sensor devices which uses wireless communications. An enormous

amount of sensor data is exchanged between the things or devices in a real time IoT scenario which needs security and privacy. Consider a health care IoT application, the patient's information is required to be confidential from the attackers. For this purpose, certain secure cryptographic algorithms are to be embedded on to the sensor devices. The following are the security requirements under data security:

a. Data Confidentiality:

Protecting sensor data from the unauthorized users provides confidentiality to the enormous data communication. Sensitive information of the IoT application like device passwords, shared encryption keys between sensor device and gateway of the network should be protected from being stolen by the hackers. Otherwise, once a device is compromised by stealing its sensitive data, the entire system can be compromised by the attacker. Hence, Data confidentiality has become an important issue in case of various IoT applications like health care monitoring, home security system.

b. Data Integrity

Data Integrity holds when the sensor data which is being communicated between various IoT devices is genuine enough and intact without any unauthorization. This also includes identity of its content as well as the source of information. This data integrity also depends on the security provided by the communication protocols being used such as 6LowPAN, MQTT in IoT applications.

c. Data Availability

In this resource constrained IoT world, several researchers found that it is very much difficult to ensure the availability of data whenever needed. Hence efforts are being carried out towards this requirement to avoid operational failures of the devices.

1.3.2 System Security

The security to be enabled in the entire system is equally important as data security. This includes various aspects like communication, devices and the network topology that is involved in the design of the system model.

a. Communication Security:

The different layers of IoT layered architecture can be made secure by using various standard communication mechanisms between the IoT devices. This can be achieved in the following ways [27]:

1. End to end security between source and destination.
2. Hop to hop security between two neighboring devices.

1.End to end security:

Among the communication protocols, IPsec present in network layer which is in transport mode provides security in the form of end-to-end basis for the system and satisfies all the security requirements. This protocol can collaborate with any one of the transport layer

protocols like TCP, HTTP, CoAP. Besides IPsec, Datagram Transport Layer Security (DTLS) is used which enforces E2E security in various applications on one machine between the transport and application layers.

2.Hop to Hop security:

The security to be enforced between two adjacent devices is hop-to-hop security. This is necessary because, in order to ensure security in communication, each node in that path are to be secure and trusted. There are many ways to implement this category of security. Message modification can be caught if there is a security check at each hop in the communication before it reaches the destination. The safety in 6LoWPAN networks is ensured if this security is incorporated so that it avoids the intruders in the radio medium wasting the system resources [5].

b. Network Security:

Apart from the communication security, there is a necessity to avoid the attackers with an aim to interfere in the availability of the network devices. The measures to be taken should be able to prevent the interruptions such as disrupting the topology with DOS attacks. Primarily, besides firewalls, an intrusion detection system is always recommended to find the intruders and their activities in the network. In addition, constant monitoring of the network by an administrator is also an important step to avoid any breach inside the network.

c. Device Security:

The addressing scheme for the devices in IoT has been one of the challenges that is constantly driving the researchers. By using IPv6 in the ever growing IoT, problems will still persist as the statistics state that the wireless IoT devices can touch 40 billion in the next decade[11]. Hence, Security at both the network as well as device levels is critical to the operation of IoT. One of the most popular application is the wearables category. There is a high chance for the hackers to attack the devices like smart watch by using the integrated motion sensor inside the watch and fabricate the critical information. Hence its high time to provide device security to prevent such ghastly attacks in IoT.

Out of which the following are the major security concerns in the context of IoT[28]:

- Authentication
- Identity Management
- User privacy
- Confidentiality
- Data Protection
- Access control and device authorization

Authentication

Lack of authentication in any network is a threat to entire system. Authentication can be the basic criteria for any user or device to get an access to the network resources. In IoT, authentication should be made as mandatory for all the devices that communicate with each other. Otherwise, the hackers can get hold of the devices which can evidently pose a threat to the network.

Identity Management

As the number of devices are roaring up high, the job of providing them unique IP addresses is also going on the tough side. Hence there is a need for efficient identity management without which the devices cannot be connected to each other via internet.

User Privacy

The details of the sensor devices present in the system should always be kept confidential. That means the privacy plays an important role in case of IoT. Privacy involves managing the critical data, reducing the probability of the attacks by using user anonymity.

Confidentiality

Confidentiality refers to the concept of hiding the crucial data from the attackers. The loads of data collected by the sensors in most of the applications like health care, home security system etc. should not go into the wrong hands which can be a threat to the user.

Data Protection

The huge amount of data generated by the devices is supposed to be under protection and should be well managed by the users. If the system lacks proper data management and protection, there is a chance of loss in the data or modification of the data by the attackers. Therefore, this is one of the security concerns in case of IoT.

Access Control and Device Authorization

Access control refers to the way the devices or users are provided with the access rights as supposed to which resources can be accessed by them. If this is not properly maintained, then even a hacker can gain access to critical resources which can be a great loss to the entire system. Further, device authorization is similar to authentication where the new devices are supposed to be authorized by the trusted entity before they gain access to the confidential resources of the network.

1.4 Authentication in IoT

To define authentication, we can say that it is a process to identify that only an authorized user is supposed to get access to the network.

Different ways of authentication are stated below:

1. based on what you know
2. based on what you have
3. based on what you are

Based on what you know

This type of authentication usually uses the values known to the user. For example, the authentication performed using the personal credentials like password, smart card, pin etc falls into this category. This type of authentication is prone to certain attacks like smart card stolen attack, password guessing attack etc.

Based on what you have

When the authentication is performed based on the entity that you possess, then it falls into this category. All the credit/debit cards, RFID tags, cryptographically secure calculators can be used as a means to participate in authentication. When

Based on what you are

This type of authentication is based on what the entity is, which means the process is carried out using the traits of the entity such as the biometric which include hand print, voice reader, scan of the retina or the signature itself.This is performed by storing the traits of the entity prior to the process. Afterwards, when he is being authenticated, a comparison is made between the actual information and the captured information.

However, there are several liabilities such as the cost effectiveness, reliability or the hacking of entity information while using this method.

The fundamental security approach for the device security in the IoT is to provide authentication and access control for the devices before the communication. Authenticating the devices will ensure the unauthorized access by the attackers in the perception layer of Internet of Things. Secure device authentication is the key requirement for the data exchange among the devices to take care of device integrity[6].

User authentication:

The entities in an IoT environment include the end customers who will utilize the data being generated by the devices from the real world. They further produce the results in the form of reports to analyze them. In order to prevent any attacker to avail this feature and eavesdrop the data, a mechanism for each and every user authentication is necessary. Before any user tries to get hold of the network device and modify or erase the data, they

must be fully authorized by the nearest gateway or base station of the network.

Device authentication:
Device authentication can prevent unauthorized users access to the Internet of things perception layer nodes and data, the effective protection of perception layer information security. At present, the main categories in authentication techniques are: authentication method based on lightweight public key algorithm, based on the pre-shared key authentication method, random key pre-distribution method of authentication and authentication method based on one-way hash function[26].

Similarly, different ways of authentication of devices in the perception layer can be categorized as follows[29]:
1. One way authentication
2. Mutual authentication

One way Authentication

When the communication among the nodes is completed by using only one message which can provide:

- The sender's identity to achieve non-repudiation.
- The receiver mentioned in the message is the actual receiver of the message.
- The message is sent as it is without any modifications while the communication takes place.

Mutual Authentication

The concept of mutual authentication came into existence to confirm that the entities participating in the communication can perform authentication with each other. When there is mutual authentication, there is no chance for the attacker to perform any impersonation attacks in the network. Usually, the sensor devices are authenticated with the base station and vice-versa to complete mutual authentication.

In the proposed method of our thesis, we used a mutual authentication procedure using password based method with variations of elliptic curve cryptography to ensure authentication between IoT devices and gateway.

1.5 Research Motivation

Internet of Things (IoT) paradigm is potentially gaining much importance day by day. The underlying elements of IoT are RFIDs, sensors and actuators which are relatively small in size and consumes less power. Various environments that have the flavor of IoT include wireless sensor networks, low-energy rate wireless personal area networks. Among

which the area that draws attention is the wireless sensor networks because of their ease of deployment in numerous real time applications[3]. Besides the several points of interest that wireless sensor networks possess like scalability, flexibility towards diverse tough conditions, they also come across certain issues like constraints on resource's energy storage capacity, vulnerability of sensor nodes towards various physical as well as other common attacks like impersonation, replay attacks[27]. Among the security challenges as defined in [5] the most important issue to be addressed is the authentication in the network. In a given environment of sensors, if the network is lacking in authentication property, there is a high level of certainty that intruders can easily fake themselves as a legitimate user and acquire critical information of the network[5]. Hence, every new external user or device who is willing to communicate with other devices present in the network should be verified if it is a legitimate device.

All the existing authentication schemes [30–32] developed for authentication are quite successful to certain extent but certain limitations still persist when using those methods. Based on their performance analysis, it can be deduced that sometimes these methods causes energy exhaustion of sensor devices and also imposes computational overhead on the network. In order to overcome such consequences of using complex authentication protocols, it is recommended to choose a light weight authentication protocol to improve the performance of sensor devices in the system.

1.6 Problem Statement and Objectives

1. Mutual authentication solution is to be proposed that minimizes the number of messages to be exchanged during authentication as well as to make it lightweight which adopts simple operations to minimize the consumption of resources in the network.

2. To design device authentication protocol for resource constrained sensor networks which are underlying technology of Internet of Things applications.

3. To evaluate the resistance of the protocols against the known active and passive attacks in perception layer of IoT.

4. To compute various performance metrics like computation time, communication overhead of the devised protocol and compare against other existing protocols.

The possible solution can be described as follows:

- The existing asymmetric algorithm solutions are memory as well as time consuming, we use variants of elliptic curve cryptography approach which provides same security with less key size,combined with symmetric system(AES) to generate the keys for

encryption of device credentials in registration and login phases of the protocol respectively and also to implement verification of device by gateway node to complete the authentication process.

- To allow secure data collection tasks between sensor device and gateway, session key agreement is to be performed using the proposed system after the authentication phase between the gateway and the device(thing).

1.7 Thesis Contribution

The major contributions of the thesis can be described as:

1. A mutual authentication with key agreement protocol is proposed for the devices to prevent unauthorized access in the network. This is carried out by a symmetric key negotiation based mechanism in order to perform a lightweight and secure mutual authentication among the devices.

2. During the symmetric key negotiation phase of the authentication process, there is a possibility of an intruder can intercept the certificate comprimising the key generation of the communication between the entities. Hence to improve its security, we further used an asymmetric key negotiation based mechanism to achieve the security as well as light weight propoerty in the mutual authentication between the devices.

1.8 Thesis Outline

In this chapter, introduction to Internet of Things, its applications, authentication problem in the context of IoT, the motivation towards the authentication problem in IoT and objectives of the research are discussed. The rest of the thesis is divided into the following chapters :

In **Chapter 2**, we discussed the security issues in perception layer, importance of authentication in the perception layer, network model, attacker model and performance metrics used.

Chapter 3 describes the proposed approach i.e.device authentication based on symmetric key negotiation with elliptic curve cryptography,comparison, results are also discussed.

Chapter 4 describes the proposed approach i.e.device authentication based on symmetric key negotiation with elliptic curve cryptography,comparison, results are also discussed.

Chapter 5 condenses the results we have acquired and presents a concise summary.

Chapter 6 describes different improvements to further enhance the performance results.

Chapter 2

Authentication in Perception Layer : Security Issues, Models

2.1 Introduction

Securing perception layer devices of IoT has been a tedious task because of their heterogeneity nature and properties such as unreliable wireless technologies, resource constraints of devices which are left in neglected environment[28]. For the security of these devices, we need to focus on various security properties. These properties can be divided into two categories- primary and secondary. The primary security properties are authentication, data availability and confidentiality along with integrity. The second category has properties such as synchronization of timestamps, data freshness and self-organization of the network. The importance of the properties varies depending on the application domain of the IoT. For example, data confidentiality and privacy is important in environmental monitoring. Authenticity, availability, integrity are crucial in health care domain[20].

IoT devices can be easily exposed to security attacks due to their deployment. Though the existing solutions for security in traditional networks are huge in number, they cannot be directly applied to IoT because of the constraints such as memory, resources, energy and its deployment in an unattended environment. This results in the need for a novel security schemes that are suitable for IoT in the context of wireless sensor networks as the nodes are not capable of performing any highly complex operations or storing any enormous data in them.

2.2 Development of WSN towards IoT

IoT consists of variety of devices with dedicated IP address interconnected globally via internet. Various IoT applications like healthcare, agriculture applications can be established by using the wireless sensor networks(WSN) based on the condition that they are able to connect to the real world devices. These IP-enabled nodes transfers the information to a central node which performs all the storage, organization of the generated huge sensor data.

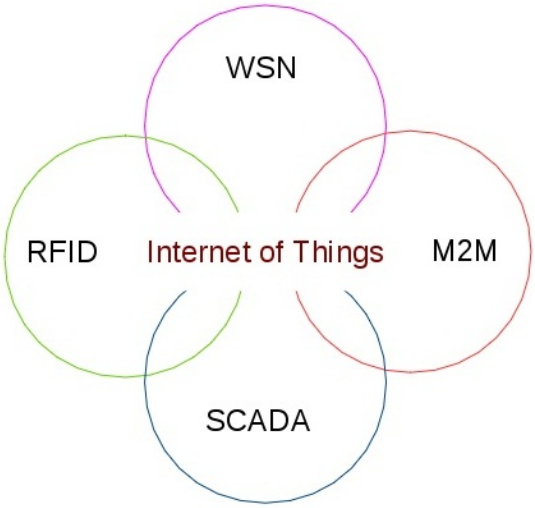

Figure 2.1: Role of WSN in IoT

This is performed by the specific gateways which are also responsible for the data flow between the devices in IoT environment. However, there arise wide range of challenges when we perform integration of WSN into IoT which include security issues, quality of service of the application and configuring the application[33].

2.3 Security Threats in Different Layers of IoT

A security threat is an act where it leverages the security weaknesses of a system and creates a negative effect on it by degrading the quality of service of the system[34].

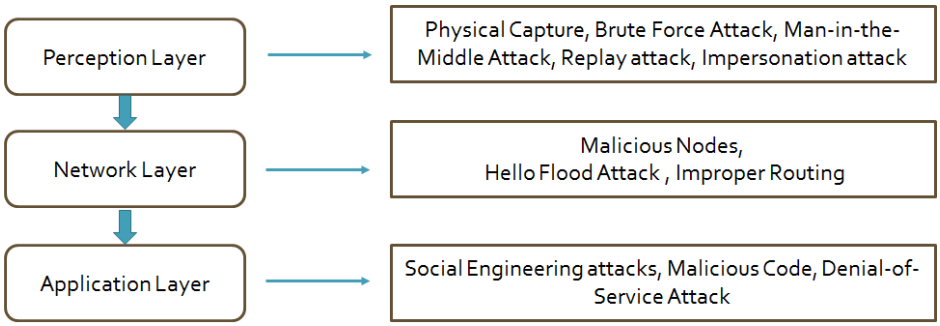

Figure 2.2: Attacks in Different Layers of IoT

Various possible attacks in different layers of IoT can be depicted in figure 2.2.

2.3.1 Security Issues in Perception Layer in IoT

Sensing layer is also called as perception layer. This layer is responsible for collecting the information and gathering the physical parameters of all the devices connected to each other. Data acquisition and collaboration are the main features of the perception layer. It has various

sensors namely temperature and humidity sensors, GPS, RFID label, camera, etc. RFID technology and sensor network technologies are the key technologies employed in this layer. Dynamic network topology and distributed nature of IoT are one of the causes for security attacks and threats [35].

The objects which are referred as 'things' in the given IoT scenario are connected to internet and hence can also suffer from various attacks by the attackers. However, various applications like health care monitoring, smart home, smart grid which incorporate the concept of Internet of Things are still suffering from plenty of vulnerabilities [2]. Recently, a study about security vulnerabilities present in IoT devices like garage door opening system revealed that any potential intruder could gain access to the device which can further lead to serious consequences like robbery. Hence security for these IoT devices has been driving the researchers to minimize the vulnerabilities and protect from plenty of attacks.

Attacks in an IoT application can be classified into the following categories [14].

1. Passive Attacks
2. Active Attacks

1. Passive Attacks:

In this type of attacks, the attackers are able to eavesdrop the data while it is being transmitted but cannot modify the data. They try to monitor the data transmission over the communication channel. Examples of these attacks are sniffing, eavesdropping.

2. Active Attacks:

In this type of attacks, the attackers not only monitors the data but also tries to perform modification of data,fabrication, interruption. Examples of these attacks are given below.

Several common kinds of attacks in perception layer are as follows[36]:

1. **Node Capture:** The perception layer devices like sensors, tags etc can be compromised by the attackers. This might result in the leakage of critical data such as the shared keys or the credentials of the nodes which can result in adverse effects on the network.

2. **Replay Attack:** The information is sent by the attacker to the receiver to gain the user's trust in the system. This is useful in authentication process, to revoke the certification of the users.

3. **Man-in-the-middle Attack:** Attacker can intercept the data collection or data acquisition tasks of the sensor devices and he can try to act as the legitimate user to acquire the critical data of the network.

4. **Impersonation Attack:** This is the attack in which the entire node's identity is being hacked by the attacker. This will result in sending false data to other nodes in the network by establishing itself as a valid node.

5. **Denial of Service Attack:** Another issue common to both IoT as well as WSN is this attack. This results in the loss of resources to attack the availability of the network services.

In order to avoid the percentage of attacks on the devices, authentication should be implemented in the network. This authentication can be external user authentication and insider or network device authentication. In a given environment of sensors, if the network is lacking in authentication property, there is a high level of certainty that intruders can easily fake themselves as a legitimate device and acquire critical information of the network[5]. Hence, every new device who is willing to communicate with other sensor nodes in the network should be verified if it is a legitimate device. Hence an authentication method is required to verify the device identity.

2.4 Related Work

The authentication protocols can be classified based on the type of cryptographic techniques used as follows:

1. Based on Symmetric Cryptography
2. Based on Asymmetric Cryptography
3. Based on Simple Hash Functions

2.4.1 Based on Symmetric Cryptography

Xue et al. proposed a novel authentication scheme based on temporal credentials along with key agreement in wireless sensor networks[32]. It manages to establish key between the user and sensor node after providing the authentication. However, in this method, user cannot change password freely. It does not restrict privileged insider attack, prone to smart card security breach attack and there is no provision of identity protection[32]. It also needs time synchronization to prevent replay attack.

An advanced password based user authentication scheme is devised which is supposed to be efficient in terms of computation cost than the existing schemes [30, 37, 38].This method comprises of four phases such as user registration, login, authentication and session key agreement, changing password which are collectively used in order to authenticate a remote user [39]. The protocol is then verified using security analysis tool which declares that the protocol allows only the valid user devices to get access rights to the sensor nodes and also achieves the authentication process in a mutual way between the gateway,the external user as well with less computational cost.

A hybrid authentication scheme with key establishment which is based on symmetric key cryptography and identity based cryptography[40]. Two protocols were proposed for

authentication and generation of pairwise and group keys for the devices in the wireless body area networks. They provide the necessary security properties but not proved to be lightweight enough during the real time implementation.

2.4.2 Based on Asymmetric Cryptography

Jiang et al. used a self-certified cryptosystem(SCK) along with Elliptic curve cryptography (ECC) in a distributed environment to perform user authentication to establish set of key pairs in sensor networks[41]. The nodes in this model which are present in the radio range of the user will try to find out if the user has proper access rights to the sensor nodes in the network. The issue with this method is that when the node receives a request for access from the user, it has to compute the pairwise keys to share with the user. It is also observed that the cost at the sensor node increase as it has to encrypt the nonce with ECC[41].

Chatterjee et al. considers wireless body area sensor networks to propose an efficient access control based method that uses a group-based user authentication method [42]. The usage of elliptic curve based public key cryptosystem enhances the access control in the network and provides a session key establishment. Results from formal analysis of the protocol mentioned that this method is safe against certain passive and active attacks. A scheme that uses elliptic curve method with lesser key size value is efficient than an authentication scheme that uses public key method with more key size[42]. Hence this method is efficient in storage wise as well as communication cost wise than other methods [30, 37]. Also, man in the middle attacks can be effectively resisted by this method with less computation complexity making it suitable for energy constrained devices.

Choi et al. proposed a protocol which is an enhancement of [42, 43]. This protocol uses elliptic curves cryptography for providing authentication for users who are trying to communicate with the sensors in the network [44]. This protocol provides resistance against sensor energy exhaustion attack, session key attack without affecting the efficiency of the protocol. It claims that considering the hash operations as negligible in calculating cost of protocol, remaining point multiplication operations performed by user, sensor and gateway node are less when compared to other protocols[42, 43] .

Debaio proposed a new authentication method which is an improved version of Yuan et al. biometric method [45]. It is an efficient method but costly biometric mechanism is deployed for providing user authentication. Further, to avoid DOS attack and impersonation attacks, an individual's unique identity which is defined by his biometric is being recorded and is further used in the registration process.

The later phases like login and authentication are also useful to computationally improve the overall performance of the method. Though this proposed method is computationally efficient, it suffers a disadvantage from cost perspective.

An ECC-based scheme which provides authentication as well as the attribute-based

access control were proposed to perform authentication in a mutual fashion between the user device and the sensor nodes.[46]. The researchers focused on the security of the perception layer devices. They had considered a third party such as attribute authority (AA) to authorize the public keys used during authentication. They had followed a clustered approach of network model to perform authentication. In addition to the authentication, the authors consider an attribute based mechanism for controlling access rights of the users. However, this method does not completely assure access control as it needs further improvements.

2.4.3 Based on Simple Hash Functions

A lightweight authentication model based on symmetric cryptographic parameters is proposed for large scale wireless networks[47]. This method uses keyed and unkeyed hash functions during the authentication process. It provides resilience against attacks such as node capture. It provides improvement in energy consumption and scalability over SPINS[48]. However, this protocol is specifically designed for large scale wireless sensor networks and hence might not be directly deployed into IoT environment.

Huang et al. proposed a method where a simple xor based encryption function is designed and used in the three phases of the authentication protocol, thereby yielding less computational cost [45]. The encryption function is a cover coded function in which the key is a generated random number and then the corresponding message to be communicated between user node and gateway node is encrypted using this key. Thus, this method claims that attacker cannot easily guess the key and intrude into the network.

A.K.Das used a simple hash function to design a robust user authentication scheme which claims to be better in terms of communication cost efficiency compared to [37, 49]. This method uses SHA-2 as a one way hash function for the purpose of providing encryption for the messages exchanged between the user and Base station, Base station and sensor node [50]. This method helps in the minimization of operations that are performed so that the computation cost is reduced. This method provides a key establishment also between user and sensor node in order to secure the communication channel. However, this method might suffer from serious attacks if the hash function is not assumed to be a random oracle model and not resistant to collision attacks [51].

A new protocol for authentication is proposed in [52] which is based on the smart cards to store the critical data of the user. The author claims that this method is suitable for constrained networks. It uses hash and exclusive or functions to establish session key between the entities.

The present methodologies which use magnetic stripe cards, smart cards are also susceptible to wide range of attacks such as duplicating the card, side channel attacks, power analysis attacks[53]. In order to execute a challenge-response based authentication protocol, a new hardware based method was introduced based on Physical Unclonable Function

(PUF). This is very effective method in terms of the response rate because it can respond to more than one cryptographic key but in a repeated manner. Each time, a new challenge response key pair is generated to perform the authentication. This technology has been applied to smart cards as well in order to counterattack the cloning attacks[54].

The author in [52] proposed a new method for authenticating user in wireless sensor networks by using the concept of IoT. This method has four phases in which the user is able to register, login, authenticate and is able to change the password. They claim that this method is resistant to DoS attacks, replay attacks but there is a security breach because of smart card. The performance analysis of this method shows that it is suitable for lightweight environment.

2.4.4 Analysis of Existing Authentication Protocol

The protocol proposed in [55] has two phases for registration and authentication. The method claims that it is lightweight and secure as they are using symmetric encryption in the authentication phase. However, in the intial registration phase, the credentials are susceptible to certain attacks like eavesdropping which can compromise the system.

In the first step of the protocol, the credentials are being sent as cleartext to the base station allowing the attacker to capture the data and impersonate himself as the valid device. Then he can calculate the shared secret value using this data. Using this value he can further calculate the constant value sent in the second message exchange to the user device. This constant value received by the device from the base station is used in the authentication phase, hence the step where the shared secret value is being captured by the attacker should be avoided.

Using which he can also interfere in the authentication phase by generating his own nonce values as a valid device and sends them to gateway for authentication. Further enhancements are suggested in the next chapters to this protocol using symmetric key negotiation and asymmetric key negotiation to avoid such attacks along with ensuring the lightweight property of the protocol.

Observations

The comparison of security features of the existing protocols that we have studied is presented in the Table 2.4.4. Most of them support mutual authentication, attack resiliency along with key agreement. But some of the protocols are not lightweight in nature which can impose overhead on the sensor devices.

Protocol	Mutual Authentication	Key Agreement	Replay Attack Resilience	Impersonation Attack Resilience	Lightweight
[32]	Yes	Yes	Yes	Yes	No
[46]	Yes	Yes	No	Yes	No
[45]	No	Yes	Yes	No	Yes
[49]	Yes	Yes	No	No	No
[52]	Yes	Yes	Yes	Yes	Yes
[56]	No	No	Yes	No	No
[50]	Yes	Yes	Yes	Yes	No

Table 2.1: Comparison of Security Features between the related schemes

2.5 Network Model

We assume that there exists two major entities: devices denoted as D and a gateway denoted as G that connects the devices to the end infrastructure via cloud as shown in the Figure 2.3. The model depicts that the devices chose the gateway to communicate with the remote servers, other services via cloud. Before they can actually communicate the data that is collected, the devices are authenticated with the gateway.

Devices are assumed to have following components:

1. It consists of hardware as well as software modules which can sense the data, form reports, receive queries, and acting accordingly. A communication system to enable wireless communications (e.g., bluetooth, zigbee) to report data to gateway and a program to process the data along with a storage space to store relevant data are available in the device.

2. It consists of software and hardware for identification of credentials and to store secrets such as keys.

Gateways are assumed to have the following properties:

1. It is an entity with secure public and private keys.

2. It is powerful enough to perform the complex operations unlike sensor device.

We focus on the authentication between the devices and the gateways. Our methods in the chapters 3,4 are applicable between the sensor devices and the smart gateway as shown

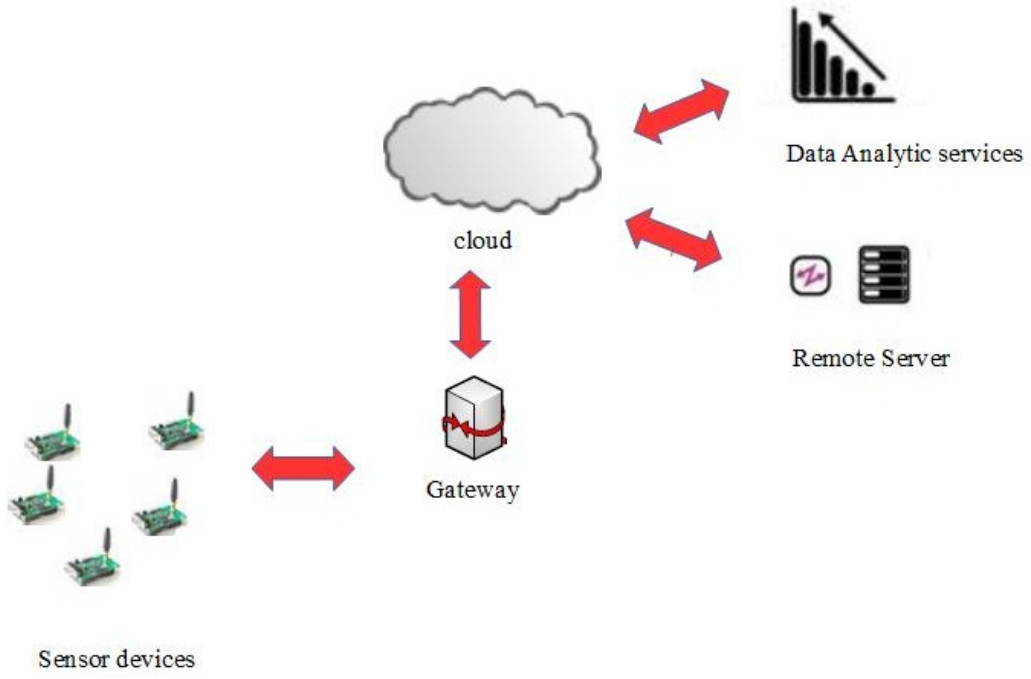

Figure 2.3: Network Model

in the figure 2.3. The sensor devices can interact with each other only after their successful authentication with the gateway of the system.

2.6 Intruder Model

The first condition to be considered is that the devices can be subjected to compromise, as they are mostly found unattended in open environments. we assume a stronger adversary which helps to provide better security, which is requirement for certain critical applications, such as health care, home security system, smart grid etc. We assume that the adversary has the ability to eavesdrop the data, send duplicate data to the devices. It is also assumed that the credentials are predefined in the device at the manufacturer.

2.7 Conclusion

In this chapter, we presented the overview of issues in the perception layer of IoT. We have also classified the security requirements and the attacks possible in perception layer of IoT. Then,we have discussed the pros and cons of various existing authentication schemes of wireless sensor networks which can be extended to our IoT system. The devices in IoT system are resource constrained like the sensor nodes in the wireless sensor networks, which needs lightweight computation based authentication methods to avoid energy depletion of the IoT devices in the perception layer. In the next chapter, we describe a new mutual device authentication method from security view point, to avoid external attacks during data

collection by simultaneously taking care of the performance metrics such as computation overhead, communication overhead as well.

Chapter 3

Device Authentication using Symmetric Key Negotiation with ECC

3.1 Introduction

IoT is always an open domain where attackers are continuously trying to hack the devices so easily. For example,hackers can gain access to the insulin pumps of the patients in case of health care and they can send false data to the hospital management. Then the staff might give false medication to the patient assuming that the data has been received from the authorized device. Hence, Authentication is one of the important security requirements for IoT devices in the perception layer of Internet of Things. However, the characteristics of the devices in the perception layer such as unattended and resource constrained nature sets the need for a secure yet lightweight authentication mechanism. Various purely symmetric and asymmetric mechanisms deal with the device authentication and access rights of the devices by using certain additional factors like smart cards, security tokens, PUF's etc. which produce nearly impeccable results in terms of security but causing overhead simultaneously. The principal factors to be considered while designing the protocols for the devices in IoT is to balance both security and overhead.

In this chapter, the authentication scheme initiates registration using an elliptic curve diffie-hellman protocol for creating a symmetric key negotiation to exchange the credentials of the device securely with the gateway. Symmetric key negotiation takes place using the ECDH protocol where both the entities exchange their public keys to arrive at a common shared symmetric key. Then it is followed by authentication where a key establishment is also performed after successfully authenticating the device. This key is further used by the devices to communicate with the gateway during data collection tasks.

3.2 Proposed Method

3.2.1 Goals

The aim of the protocol is to achieve device authentication and secure key establishment with the common key to be used in the next stage of communication between the devices. Besides, there are other security goals to be achieved such as the resistance against the perception layer attacks such as impersonation attack, replay attacks while preserving the integrity,availability.

3.2.2 Assumptions

- It is assumed that the attacker is able to eavesdrop the messages between the two entities.
- The attacker can impersonate any one of the entities.
- The secrets which are pre-defined inside both the devices are safe from the attacker.

3.2.3 Protocol Definition

The protocol consists of two participants - IoT device and gateway/base station. The notations used in the proposed method are given in the Table 3.2.3. The proposed method performs authentication in two phases described as follows.

1. Device Registration
2. Device Authentication

Preliminaries of Elliptic Curve Diffie Hellmann(ECDH)

When the Diffie-Hellman protocol is added the flavor of elliptic curves, a key agreement protocol called Elliptic Curve Diffie-Hellman is evolved. The main function of this method is to ensure the two entities generate their own key pairs. Then agree to a common secret which is generated by exchanging the key pairs over the communication channel. This channel can be any insecure one which is an added advantage to the users of the public medium in the communication. The combination of the elliptic curve cryptography which is an asymmetric system with the symmetric diffie-hellman resulted in this method. The final shared key is used for encryption between the two parties as how it is used in traditional diffie-hellman algorithm. This key can also be used to produce another key as per the constraints.

The parameters which are used to calculate the key pairs are basically a very long prime number p along with another integer g with a condition $g < p$. Firstly, these details are exchanged by both the parties over in an insecure medium. Then they choose their own

Symbol	Meaning
v	Secret Value of the system
$\|$	Concatenation
N_d	Random nonce of the device
$\oplus$	Exclusive OR
N_g	Random nonce of the gateway
D_k	Shared key generated using Diffie-Hellman
H(.)	One-way hash Function
$E(M, K)$	Encryption function of M with key K

Table 3.1: Notations

private integers a , b which are called private key of them. Further, they use the received parameters and their private key to generate their own public keys. The common key generated by both parties will match but not their private keys. The commonly shared key in this case would be $g^a modp$ for the user A and $g^b modp$ for the user B.

The secret key is calculated from their private keys. Thus if an eavesdropper captures the values p, g , he cannot find the secret key with the knowledge of only their public keys. Hence, this protocol is said to be secure until the attacker is not able to solve the hardest Elliptic curve discrete logarithmic issue. The usage of shorter keys in case of this method fetches the same level of security as RSA which uses larger keys. This is because of the elliptic curves used in this system.

Device Registration

In this phase, the IoT device and the gateway are initialized with the required predefined security parameters. When the new device enters the network, it is first registered at the gateway before performing any data collection functions. A secret value v is generated by the intermediate gateway in order to perform authentication and registration of the new devices. Every new device performs this registration phase before it tries to communicate with the other devices of the network. This phase starts with the exchange of device identity and password with the gateway.

Firstly, the device and the gateway will undergo the process of key negotiation using the Elliptic Curve Diffie-Hellman(ECDH) to securely transfer the device credentials to the gateway as shown in the Figure 3.1. A symmetric key is established between the two entities

to complete the registration phase. This helps to avoid any eavesdropping by the attackers while transferring the device credentials.

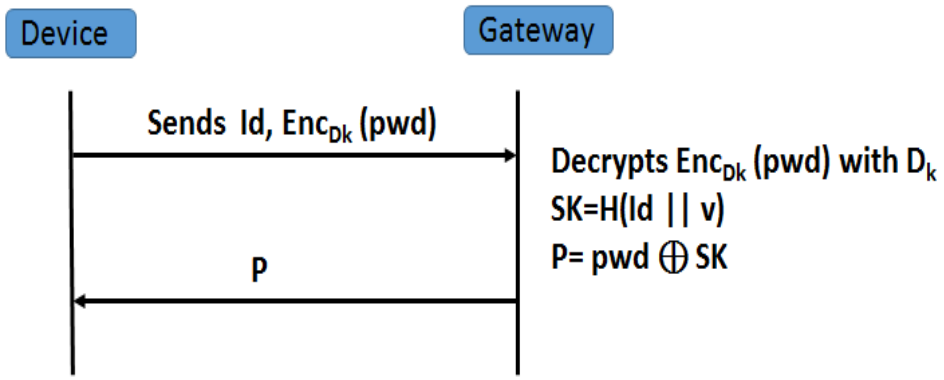

Figure 3.1: Device Registration Phase

The following steps are followed accordingly by both device and gateway in order to complete the registration phase as described in the below algorithm 3.1.

Step 1: The device encrypts its credentials i.e., identity (id) and password (pwd) with the available shared symmetric key D_k generated using the symmetric key negotiation before sending it to gateway.

Algorithm 3.1 Device Registration Phase

1: $D \rightarrow G$: Sends Id and $E_{Pu_k}(pwd)$, Password pwd encrypted with Elliptic Curve Diffie-Hellman symmetric key D_k

2: G : Decrypts the message to find the password pwd and Computes the shared secret value SK = H ($Id \parallel V$), $P = SK \oplus pwd$

3: $G \rightarrow D$: Sends P

Step 2: The gateway then decrypts the arrived encrypted message with its own symmetric key (D_k) and computes the following: i) Secret key SK= H(id $\parallel$ v) where $\parallel$ is concatenation operation ,H is a one-way hash function. ii) a new value P = pwd $\oplus$ SK where $\oplus$ is exclusive or operation. Then this new value P is registered with the device which is later used by it in the authentication stage of the device.

Device Authentication

In order to communicate with other devices and perform its tasks securely, a device needs to login and authenticate with the gateway of the network. After successfully being registered at the gateway, the device will go through the authentication process when it tries to acquire access to the other devices as shown in Figure 3.2.

This process is carried out using the p value stored in the registration part of the device. Only three message exchanges takes place to ensure the successful operation. This helps to scale down the consumption of resources of the device. If the device is unable to produce

the same values as exchanged in the previous registration stage, then the process termination will takes place.

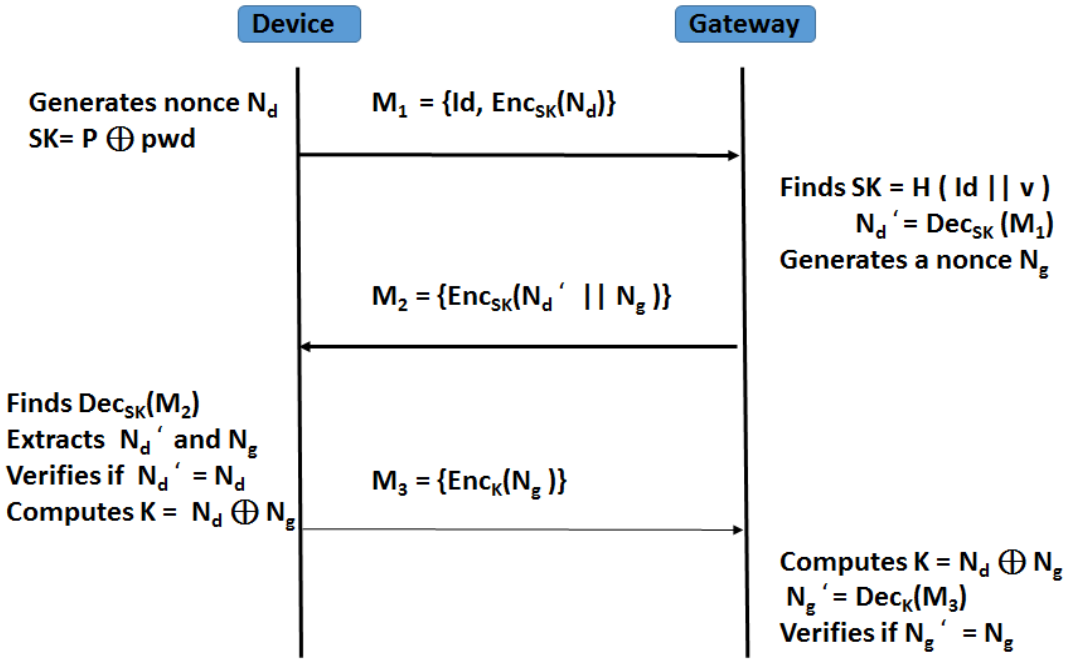

Figure 3.2: Device Authentication Phase

The process is started by following steps which are carried out as follows :

Step 1 : The device starts this phase by computing the secret key SK by using the registered P value and its password (pwd) as $SK = P \oplus pwd$. Then it generates a nonce N_d which is a random number and sends the message $M1 = id, (Nd)SK$ to gateway which has device id and encrypted value of the random number N_d using advanced encryption standard (AES) symmetric key encryption with the secret key SK. This AES encryption is useful in low-rate personal area networks which contain battery operated devices.

Step 2 : After the gateway receives message $M1$, the gateway computes the necessary values SK which is calculated by $SK = H(id||v)$. Further, the gateway also decrypts the received message M1 using this calculated secret key SK for the device's random value N_d. Then the gateway also generates his own challenge by generating his own random number N_g.

Using the secret key SK, gateway sends an encrypted message $M2 = (N_d||N_g)_{SK}$ to the device.

Step 3 : After the arrival of the message $M2$ from the gateway, the device starts decrypting the message using the secret key SK to find the nonce values N_d,N_g. After further verification of both the sent and received Nd, the device then calculates the session key $K = N_d \oplus N_g$. This ensures the authenticity of the gateway with the device if the verification is successful.

Then the received N_g value is encrypted using this key K and then sent as message $M3$ to the gateway.

Step 4 : When the message arrives, the gateway immediately computes the key $K = N_d \oplus N_g$ and decrypts the message using this session key. The decrypted message N_g is then verified by the gateway with its own N_g. This will complete the authentication of the device with the gateway if the verification is successful. Otherwise the communication is terminated with the device.

The session key K, which is established during the authentication stage can be used by the device and gateway during the data management tasks like data collection and data acquisition or any other task performed by the device.

Algorithm 3.2 Device Authentication Phase

1: D : Generates random number N_d, Computes $SK^{'} = P \oplus pwd$
2: $D \rightarrow G$: Message $M1 = Id, E_{SK'}(N_d)$
3: G : Computes $SK = h(Id\|v)$, $N_d^{'}$ by decrypting $E_{SK'}(N_d)$ with SK, generates random number N_g
4: $G \rightarrow D$: Message $M2 = E_{SK}(N_d^{'}\|N_g)$
5: D : recovers $N_d^{'}$, $N_g^{'}$ by decrypting $M2$ using $SK^{'}$, verifies $N_d = N_g^{'}$ and computes session key $K = N_d \oplus N_g^{'}$
6: $D \rightarrow G$: Message $M3 = E_{SK'}(N_g^{'})$
7: G : recovers $N_g^{'}$ by decrypting $M3$ using SK and verifies $N_g = N_g^{'}$, Computes session key $K = N_d^{'} \oplus N_g$

The above algorithm describes the authentication phase of the device with the gateway where a nonce N_d is generated by the device to compute the shared key value and sends the message $M1$ to gateway. Then the gateway also generates N_g and sends message $M2$ to the device. Further, both of them verify the integrity of the received nonces and generate a session key if the authentication of the device is successful.

3.3 Security Analysis

The protocol is said to be secure if it is able to resist against external active and passive attacks. In this protocol, the secret value v is to be kept safe which provides the necessary security to the system. This value is generated as a complex random value in order to avoid any brute force attack to guess it which is not desirable. The proposed protocol is said to be secure against the following list of attacks.

1. Impersonation Attack :

Impersonation attack is said to be present if the attacker is able to compromise the device or the gateway during the communication. This is not possible in both the stages because the key SK is unknown to the attacker and it is not possible to be revealed at any point. Hence it is difficult for the intruder to find the nonce values from the captured messages $M2$ and generate the message $M3$. Hence he cannot complete his authentication process.

2. Replay Attack :

Replay attack occurs when the attacker tries to capture the message over the communication channel and uses the same message to prove his identity. This is not possible in the authentication stage of the protocol because if the attacker tries to capture the messages, he cannot evaluate the same new nonce value N_g or N_d from the intercepted messages.

3. ECDH limitation

The ECDH key exchange protocol used in the device registration is said to be prone to man in the middle attack. This disadvantage is because of the static keys used in the scheme which can be predictable at times and also it lacks pre-verification of the entities. The attacker can eavesdrop the data when the keys are exchanged to produce a shared symmetric secret for the encryption of the device credentials as shown in the Figure 3.3.

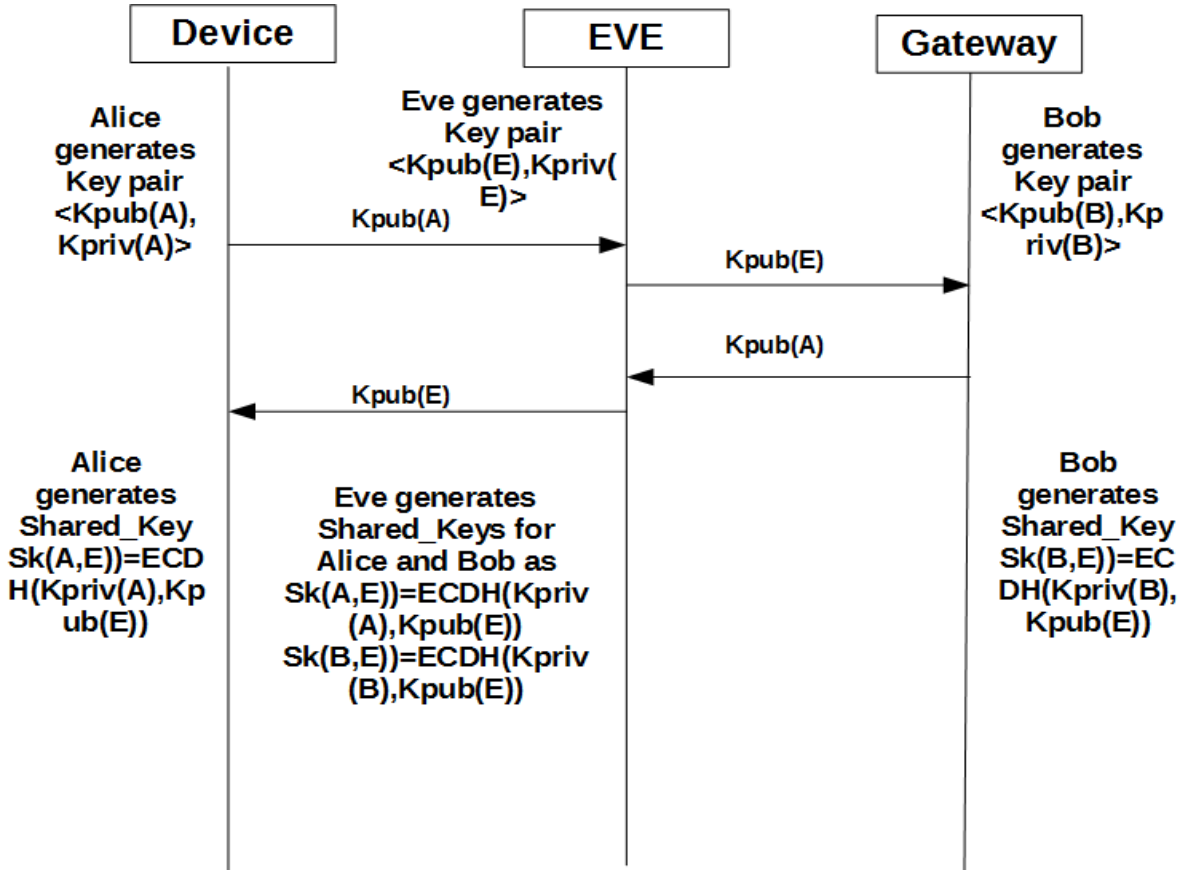

Figure 3.3: Man-in-the-middle Attack in ECDH

Thus the protocol is not resilient to man-in-the-middle attack which is a possible attack in the first step of device registration stage because of the implementation of Elliptic Curve Diffie-Hellman cryptosystem. Hence, an improvement is necessary in this phase to avoid this attack and improve the security of the protocol.

The protocol not only provides resistance to above attacks but also provides the following security requirements.

1. Mutual Authentication

There is a need for mutual authentication in order to ensure the authenticity of both user devices as well as the sink node or gateway. This protocol ensures this mutual authentication by the nonces(N_d, N_g) generated by both the entities of the communication. This also helps to prevent any chances of impersonating the sink node or gateway as there is a possibility that the attacker might impersonate the gateway or sink node in order to send the fake data to user devices. Therefore, mutual authentication ensures the authenticity of the sources that are generating data during communication.

2. Session key Agreement

The last step of this protocol is to establish a secret key $K = N_d \oplus N_g$ between the device and the gateway/sink node. The generated session key is useful further in the communication among the devices i.e.,the device and the gateway/sink node or any two devices.

3.4 Simulation Analysis

The Contiki operating system is a C based OS designed for embedded systems lightweight and capable of multitasking. It is highly memory efficient and open source, allowing custom modifications and improvements from a wide community. It is capable of dynamic application loading and unloading capabilities for services and applications. This gives it numerous advantages in terms of resource utilization and allows a highly efficient kernel driven architecture for sensor networks. This makes it an ideal operating system for implementation of our scheme of secure authentication using symmetric and asymmetric cryptography techniques.

The proposed protocol is implemented for the Contiki environment using the Java programming language. In order to implement the device registration phase of the protocol, cryptographic provider libraries such as FlexiProvider and bouncy castle are used. Similarly to implement the authentication phase of the protocol, we used the AES protocol implementation provided in the bouncy castle library.

It is then simulated in Cooja simulator under Contiki OS environment. For the simulation, we loaded the programming code of IoT device process on one mote and code of gateway process on the second mote and recorded the execution time of the interaction of both the phases of the protocol .

Operating System	Languages Supported	Memory Required(Kb)	Event Based Programming
TinyOS	nesC	1	Yes
Contiki	C,Java	2	Yes
LiteOS	C	4	Yes
RiotOS	C/C++	1.5	No

Table 3.2: Operating Systems Mostly Used in IoT Environment

3.4.1 Performance Metrics

Metrics are a measure for calculating and estimating the effectiveness of the protocols. The factors which are used to measure the lightweight property of the protocol are mentioned below. This protocol is evaluated using the following performance metrics :

1. Computation Cost
2. Communication Cost
3. Execution Time

1. Computation Cost

The constrains of IoT resource-limited devices have been taken into account while designing the protocol, hence, all the operations employed in our protocol are simple and lightweight as a complaint with this requirement. This is the combination of time taken by all the operations carried out in the protocol.

T_H: the execution time of a one-way hash function

T_{MUL}: the execution time for an ECC point multiplication

T_{D_ENC}:time required to execute the Diffie-Hellman key encryption.

T_{ENC}:time required to execute the symmetric key encryption.

T_{DEC}:time required to execute the symmetric key encryption.

Protocol	Computation cost
Proposed Protocol	$1T_{MUL} + 1T_{D\_ENC} + 2T_{ENC} + T_{DEC}$
Choi et al. [44]	$4T_H + 3T_{MUL}$
Chatterjee et al. [42]	$3T_H + 2T_{MUL} + 3T_{DEC}$

Table 3.3: Comparison of Computation Cost at device

2.Communication Cost

Communication costs refer to the number of the messages exchanged between the Claimer and the Verifier during the authentication process and also the size of each message in bytes.

Protocol	Communication cost
Proposed Protocol	3 messages
Choi et al. [44]	6 messages
Chatterjee et al. [42]	6 messages

Table 3.4: Comparison of Communication Cost of Protocol

3. Execution Time

This metric can be defined as the time taken for the successful completion of the protocol.

Total Execution Time(in seconds) = $T_{Reg} + T_{Auth}$

T_{Reg} : Time to execute registration phase of protocol

T_{Auth} : Time to execute authentication phase of protocol

The registration stage takes 0.278s to execute as we have used ECDH. The authentication process is executed in 0.211s. Hence the total time for the execution of the protocol is 0.489s as shown in table 3.4.1.

3.5 Conclusion

A mutual authentication protocol using symmetric design for the unattended devices of perception layer of IoT is discussed. This device authentication protocol can address

Protocol	Execution Time(s)
Proposed Protocol	0.489s
Choi et al. [44]	2.102s
Chatterjee et al. [42]	6.018s

Table 3.5: Comparison of Execution Time with Different Protocols

the problems of the former schemes and provide better security and slims down the cost overhead. This scheme allows the device as well as the sink/gateway to authenticate with each other thus preventing impersonation and replay attacks. After successful authentication, secure data collection tasks can be performed by the devices with the help of the calculated session key between them. However, there persist the man-in-the-middle attack in the registration phase of the protocol which can be avoided using an asymmetric design which is discussed in the next chapter.

Chapter 4

Device Authentication using Asymmetric Key Negotiation with ECC

4.1 Introduction

The enormously evolving ubiquitous and resource constrained devices have generated the urge to enhance the levels of security as well as improve the numbers of the performance parameters of their protocols. The protocols designed for different layers of IoT satisfy different set of security requirements. Further, the effect of attackers can be avoided by using asymmetric key cryptography rather than symmetric key cryptography. The difference between both of them is that in case of symmetric key cryptography, better performance is observed with possibility of attacks. Because symmetric key cryptosystem uses an identical private key to encrypt and decrypt messages. The private key consists of numbers, words and billions of character strings. In this cryptosystem, both a message sender and a message receiver shares an identical private key for encryption and decryption. Once the private key is stolen or unintentionally disclosed, anyone can decrypt the encrypted message. While in case of asymmetric key cryptography, a trade-off between security and performance of the protocols can be observed.

The proposed method in previous chapter is based on the ECDH where the keys are generated by the device and gateway prior to the communication. Such keys are not ephemeral type and hence they are called static keys. These keys that are generated each time separately are called ephemeral keys. For this purpose, one needs to trust the public keys of both the key pairs to utilize them in further authentication. In order to avoid the attacks caused by this static nature of these keys, we propose a solution for this problem by using an Integrated encryption scheme where the key pair is computed at gateway side only which results in less computation overhead as the key pair generation is skipped for the device.

4.2 Proposed Method

4.2.1 Goals

The aim of the protocol is to achieve device authentication and secure key establishment with the common key to be used in the next stage of communication between the devices. Besides, there are other security goals to be achieved such as the resistance against the perception layer attacks such as impersonation attack, replay attacks while preserving the integrity,availability.

4.2.2 Assumptions

- It is assumed that the attacker is able to eavesdrop the messages between the two entities.
- The attacker can impersonate any one of the entities.
- The secrets which are pre-defined inside both the devices are safe from the attacker.

4.2.3 Protocol Definition

The protocol involves two participants - IoT device and gateway/base station. The proposed method consists of two stages- registration stage with asymmetric key negotiation , authentication phase with symmetric key establishment.

1. Device Registration
2. Device Authentication

Preliminaries of Elliptic Curve Integrated Encryption Scheme(ECIES)

ECIES is the integrated encryption scheme based on elliptic curves which is a combination of public key functions, encryption algorithms with codes for hashing and authentication. Briefly, this scheme is the generic scenario used to find a set of variants in encryption schemes. In this scheme, the server will generate its key pairs using a specified curve. It then sends the public key in a standard encoding format such as X.509 or ANSI X9.63 to the client. On the client side, the protocol uses the public key from the server to generate the secret information like secret MACs and key material necessary for the encryption process. Finally it sends the encrypted cryptogram to the server where the server can use its private key to recover the cleartext from the cryptogram.

Symbol	Meaning
v	Secret Value of the system
$\|$	Concatenation
id	id of the device
pwd	password of the device
N_d	Random nonce of the device
$\oplus$	Exclusive OR
N_g	Random nonce of the gateway
H(.)	One-way hash Function
PU_k	Public Key of the gateway generated using ECIES
PR_k	Private Key of the gateway generated using ECIES
E(M,K)	Encryption function of M with key K
D(M,K)	Decryption function of M with key K

Table 4.1: Notations

Device Registration

In this phase, the IoT device and the gateway are initialized with the required predefined security parameters. When the new device enters the network, it is first registered at the gateway before performing any data collection functions as shown in Figure 4.1. A secret value v is generated by the intermediate gateway in order to perform authentication and registration of the new devices. Every new device performs this registration phase before it tries to communicate with the other devices of the network. This phase starts with the exchange of device id and password with the gateway. The following steps are followed accordingly by both device and gateway in order to complete the registration phase as shown in figure 4.1.

Step 1: The device encrypts its credentials i.e., identity (id) and password (pwd) with the available public key of the gateway(PU_k) before sending it to gateway.

Step 2: The gateway then decrypts the arrived encrypted message with its own private key (PRk) and computes the following: i) Secret key SK= H(id || v) where || is concatenation operation ,H is a one-way hash function. ii) a new value P = pwd $\oplus$ SK where $\oplus$ is exclusive

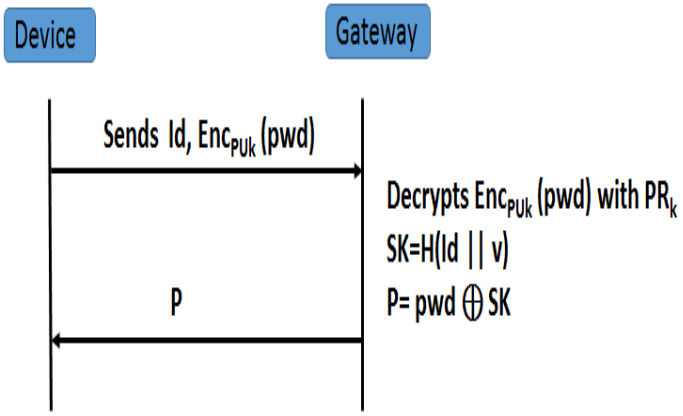

Figure 4.1: Registration Phase

or operation. Then this new value P is registered with the device which is later used by it in the authentication stage of the device.

Algorithm 4.1 Device Registration Phase.

1: $D \rightarrow G$: sends Id and $E_{Pu_k}(pwd)$, Password pwd encrypted with public key Pu_k of gateway.
2: G : Computes the shared secret value SK = H ($Id \parallel V$), $P = SK \oplus pwd$
3: $G \rightarrow D$: sends P

In the above algorithm 4.1, after the asymmetric key negotiation, the device acquires the public key of the gateway to send its encrypted credentials. After decrypting the message to get the password, the gateway calculates the value of P using the device credentials and sends it to the device which completes the registration phase.

Device Authentication

In order to communicate with other devices and perform its tasks securely, a device needs to login and authenticate with the gateway of the network.
The process is started by following steps which are carried out as follows :

step 1 : The device starts this phase by computing the secret key SK by using the registered P value and its password (pwd) as $SK = P \oplus pwd$. Then it generates a nonce N_d which is a random number and sends the message $M1 = id, (Nd)SK$ to gateway which has device id and encrypted value of the random number N_d using AES symmetric key encryption with the secret key SK. This AES encryption is useful in low-rate personal area networks which contain battery operated devices.

Step 2 : After the gateway receives message M1, the gateway computes the necessary values SK which is calculated by $SK = H(id \| v)$. Further, the gateway also decrypts the received message M_1 using this calculated secret key SK for the device's random value N_d. Then the gateway also generates his own challenge by generating his own random number

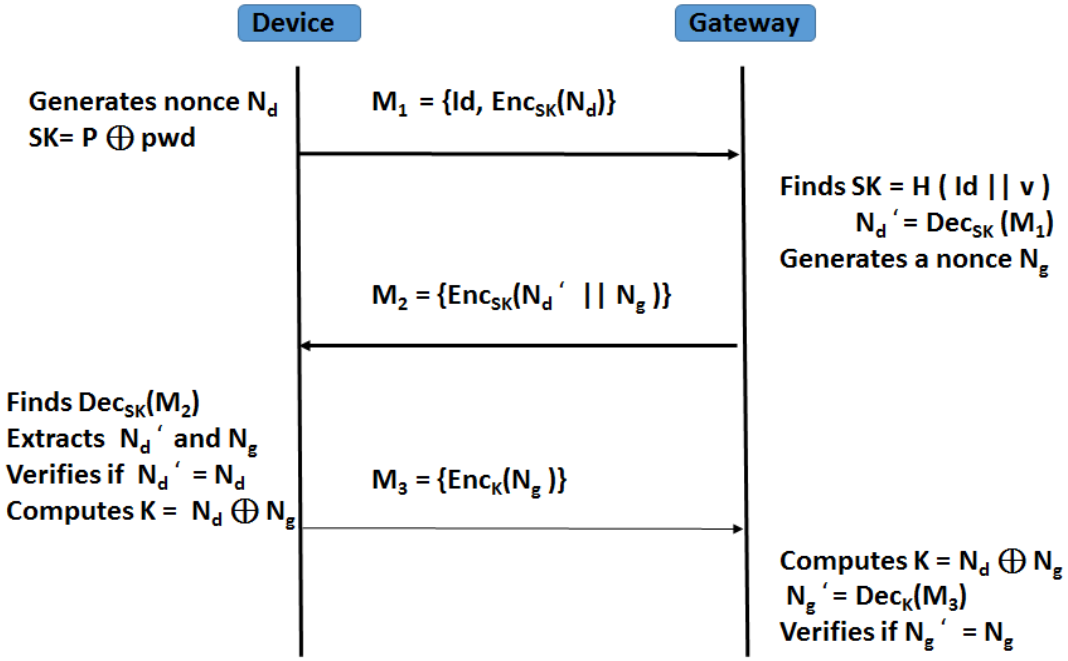

Figure 4.2: Authentication Phase

N_g.

Using the secret key SK, gateway sends an encrypted message $M_2 = (Nd||Ng)SK$ to the device.

Step 3 : After the arrival of the message M_2 from the gateway, the device starts decrypting the message using the secret key SK to find the nonce values N_g, N_g. After further verification of both the sent and received Nd, the device then calculates the session key $K = N_d \oplus N_g$. This ensures the authenticity of the gateway with the device if the verification is successful.

Then the received N_g value is encrypted using this key K and then sent as message M_3 to the gateway.

Step 4 : When the message arrives, the gateway immediately computes the key $K = N_d \oplus N_g$ and decrypts the message using this session key. The decrypted message N_g is then verified by the gateway with its own Ng. This will complete the authentication of the device with the gateway if the verification is successful. Otherwise the communication is terminated with the device.

The session key K, which is established during the authentication stage can be used by the device and gateway during the data management tasks like data collection and data acquisition or any other task performed by the device.

Algorithm 4.2 Device Authentication Phase

1: D : Generates random number N_d, Computes $SK^{'} = P \oplus pwd$
2: $D \rightarrow G$: Message $M1 = Id, E_{SK'}(N_d)$
3: G : Computes $SK = h(Id\|v)$, $N_d^{'}$ by decrypting $E_{SK'}(N_d)$ with SK, generates random number N_g
4: $G \rightarrow D$: Message $M2 = E_{SK}(N_d^{'}\|N_g)$
5: D : recovers $N_d^{'}$, $N_g^{'}$ by decrypting $M2$ using $SK^{'}$, verifies $N_d = N_g^{'}$ and computes session key $K = N_d \oplus N_g^{'}$
6: $D \rightarrow G$: Message $M3 = E_{SK'}(N_g^{'})$
7: G : recovers $N_g^{'}$ by decrypting $M3$ using SK and verifies $N_g = N_g^{'}$, Computes session key $K = N_d^{'} \oplus N_g$

In the above algorithm 4.2, the authentication process of the device is carried out with the gateway in a mutual fashion. Both the entities exchange the encrypted one time generated nonce values with each other by using a symmetric key system. If the received nonce values are valid, then the authentication is said to be performed successfully.

4.3 Security Analysis

The protocol is said to be secure if it is able to resist against external active and passive attacks. In this protocol, the secret value v is to be kept safe which provides the necessary security to the system. This value is generated as a complex random value in order to avoid any brute force attack to guess it which is not desirable. The proposed protocol is said to be secure against the following list of attacks.

1. Impersonation Attack : Impersonation attack is said to be present if the attacker is able to compromise the device or the gateway during the communication. This is not possible in both the stages because the key SK is unknown to the attacker and it is not possible to be revealed at any point. Hence it is difficult for the intruder to find the nonce values from the captured messages $M2$ and generate the message $M3$. Hence, the intruder cannot complete his authentication process.

2. Replay Attack : Replay attack occurs when the attacker tries to capture the message over the communication channel and uses the same message to prove his identity. This is not possible in the authentication stage of the protocol because when the attacker tries to capture the messages, he cannot evaluate the same new nonce value N_g or N_d each time from the corresponding messages.

3. Man-in-the-Middle Attack : This attack usually occurs when an outsider is able to capture the information and attempts to change the communication between sender and receiver.

As we have incorporated the asymmetric key negotiation using Elliptic Curve Identity Encryption Scheme(ECIES) in the beginning phase of the protocol, it is not so easy for the attacker to perform this attack.

The protocol not only provides resistance to above attacks but also provides the following security requirements.

1. Mutual Authentication

There is a need for mutual authentication inorder to ensure the authenticity of both user devices as well as the sink node or gateway. This protocol ensures this mutual authentication by the nonces(N_d, N_g) generated by both the entities of the communication. This also helps to prevent any chances of impersonating the sink node or gateway as there is a possibility that the attacker might impersonate the gateway or sink node in order to send the fake data to user devices. Therefore, mutual authentication ensures the authenticity of the sources that are generating data during communication.

2. Session key agreement

The last step of this protocol is to establish a secret key $K = N_d \oplus N_g$ between the device and the gateway/sink node. The generated session key is useful further in the communication among the devices i.e.,the device and the gateway/sink node or any two devices.

4.4 Simulation Analysis

The Contiki operating system is a C based OS designed for embedded systems lightweight and capable of multitasking. It is highly memory efficient and open source, allowing custom modifications and improvements from a wide community. It is capable of dynamic application loading and unloading capabilities for services and applications. This gives it numerous advantages in terms of resource utilization and allows a highly efficient kernel driven architecture for sensor networks. This makes it an ideal operating system for implementation of our scheme of secure authentication using symmetric and asymmetric cryptography techniques.

The proposed protocol is implemented for the Contiki environment using the Java programming language. In order to implement the device registration phase of the protocol, cryptographic provider libraries such as FlexiProvider and bouncy castle are used to implement Elliptic Curve Integrated Encryption Scheme (ECIES). Similarly to implement the authentication phase of the protocol, we used the AES protocol implementation provided in the bouncy castle library.

It is then simulated in Cooja simulator under Contiki OS environment. For the simulation, we loaded the programming code of IoT device process on one mote and code of gateway process on the second mote and recorded the execution time of the interaction of both the phases of the protocol .

4.4.1 Performance Metrics

This protocol is evaluated using the following performance metrics :

1. Computation Cost

The constrains of IoT resource-limited devices have been taken into account while designing the protocol, hence, all the operations employed in our protocol are simple and lightweight as a complaint with this requirement.

T_H: the execution time of a one-way hash function

T_{MUL}: The execution time for an ECC point multiplication

T_{sign}: The execution time for generating signature.

T_{ENC}: Time required to execute the symmetric key encryption.

T_{PU_ENC}: Time required to execute the Public key encryption.

T_{DEC}: Time required to execute the symmetric key decryption.

Protocol	Computation cost
Proposed Protocol	$T_{PU\_ENC} + 2T_{ENC} + T_{DEC}$
Zhao's Protocol [57]	$2T_H + 3T_{MUL} + T_{sign}$
Chatterjee's Protocol [42]	$3T_H + 2T_{MUL} + 3T_{DEC}$

Table 4.2: Comparison of Computation Cost at device

2.Communication Cost

Communication costs refer to the number of the messages exchanged between the Claimer and the Verifier and also the size of each message in bytes.

Protocol	Communication cost
Proposed Protocol	3 messages
Zhao's Protocol [57]	5 messages
Chatterjee's Protocol [42]	6 messages

Table 4.3: Comparison of Communication Cost of Protocol

3. Execution Time

This metric can be defined as the time taken for the successful completion of the protocol. Total Execution Time(in seconds) = $T_{Reg} + T_{Auth}$

T_{Reg} : Time to execute registration phase of protocol
T_{Auth} : Time to execute authentication phase of protocol
The registration stage takes 107ms to execute as we have used ECIES. The authentication process is executed in 211ms. Hence the total time for the execution of the protocol is 378ms.

Protocol	Execution Time(s)
Proposed Protocol	0.378s
Zhao's Protocol [57]	4.807s
Chatterjee's Protocol [42]	6.018s

Table 4.4: Comparison of Execution Time with Different Protocols

4.5 Case Study

The proposed protocols can likely be deployed in the following scenario of wireless body area network which is also one of the technologies that incorporates IoT.

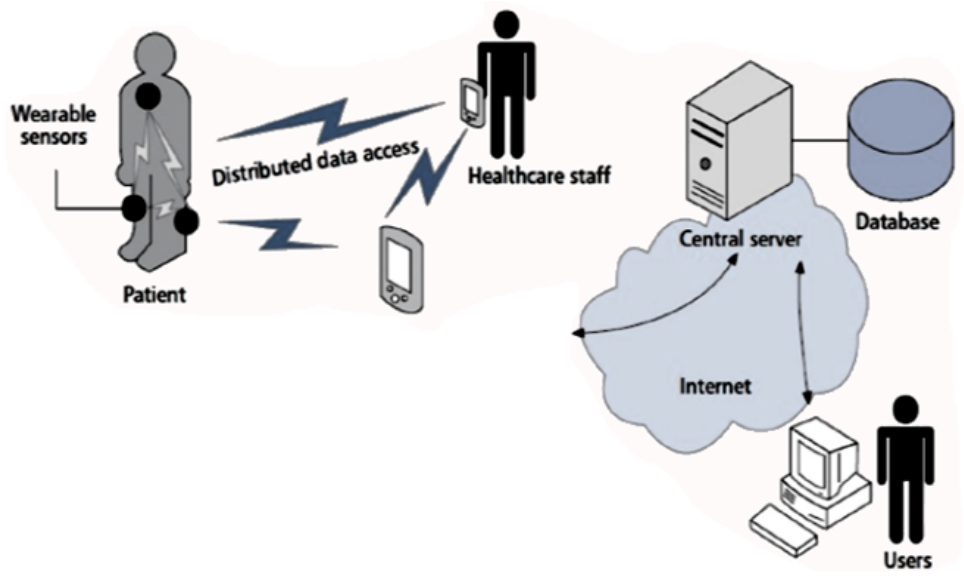

Figure 4.3: Deployment Scenario

The patient's sensor will communicate with the health care staff via the gateway as shown in Figure 4.3. When there is any alert given by the patient's device to the health care staff for any emergency, the medication details are immediately communicated to him. But if the attacker gains access to the patient's device, he can send false alerts to the staff resulting in

the false medication provided to the patient which is a deadly risk for the patient. Hence, an authentication mechanism should be incorporated between the patient's device and the gateway before it communicates with the staff. Similarly, the staff's device should also be authenticated before they send any medication information to the patients.

Our assumed device in the proposed protocol can be patient's device or staff device and the gateway in our protocol is the server shown the Figure 4.3. After the authentication is performed, using the session key both the entities can exchange valid information with each other with less computation cost as our protocols are supposed to be lightweight in nature.

4.6 Conclusion

A mutual authentication protocol using asymmetric design for the unattended devices of perception layer of IoT is elaborated. This device authentication protocol can address the problems of the former schemes as well as the scheme which was discussed in previous chapter in terms of security and cost overhead. This mutual authentication scheme prevents impersonation and replay attacks as well as man-in-the-middle attacks. After successful authentication, secure data collection and acquisition tasks as applicable to the perception layer can be performed by the devices, by using the established secret session key between the device and the gateway of the system. The simulation analysis reveals that the proposed system performs better in terms of the three performance metrics considered such as execution time, computation cost, communication cost. This method requires only 3 message exchanges for completing the authentication process in 0.378s with simple symmetric encryption and XOR functions.

Chapter 5

Conclusion

In thesis, we mainly focused on the security challenges of IoT. we then addressed the problem of authentication in perception layer of IoT. We observed that the existing authentication methods are still subjected to attacks and some of them produce overhead at the device.

Hence, in the chapter 3, we proposed a symmetric key negotiation based authentication mechanism which uses Elliptic Curve Diffie-Hellman in the registration phase and a symmetric key establishment is performed at the end of authentication phase of the protocol. This key is then used between the devices for data collection tasks. We can observe that mutual authentication is achieved. Based on the performance analysis, the proposed method is also lightweight compared to the existing methods due to the smaller key size used by the ECC cryptography. But in security analysis, we observed that the protocol can be subjected to man-in-the-middle attacks.

Hence,in the chapter 4,we proposed an asymmetric key negotiation based authentication mechanism which uses Elliptic Curve Integrated Encryption Scheme in the registration phase and a symmetric key establishment is performed at the end of authentication phase of the protocol. This key can be used between the devices for data collection tasks. We can observe that mutual authentication is achieved in this method. Based on the performance analysis, the proposed method is also lightweight compared to the existing methods but we can observe a tradeoff between security and lightweight factor.

Further, it is recommended to put efforts in this direction to improve these methods with certain level of standards which aims at light weight nature and security within the IoT infrastructure.

Chapter 6

Future Work

In thesis, authentication for perception layer sensor devices is performed using symmetric and asymmetric key negotiation in the registration phase of the device. Informal security analysis is also performed against various active and passive attacks such as impersonation, replay, man-in-the-middle attacks. Mutual Authentication using password based method in the proposed protocol can be further enhanced by using methods that will not involve password of the device to avoid device stolen attacks.

In the process of simulating the protocol in Cooja simulator, we considered only cooja motes to emulate the protocol. In future work, different motes like skymote, zolertia etc can be used as test beds and also the protocol is supposed to be implemented in the real hardware.

Bibliography

[1] M. H. Rehmani and A.-S. K. Pathan, *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*. CRC Press, 2016.

[2] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[4] E. Sazonov and M. R. Neuman, *Wearable Sensors: Fundamentals, implementation and applications*. Elsevier, 2014.

[5] A. Blilat, A. Bouayad, N. el houda CHAOUI, and M. Ghazi, "Wireless sensor network: Security challenges," in *Network Security and Systems (JNS2), 2012 National Days of*. IEEE, 2012, pp. 68–72.

[6] K. Zhao and L. Ge, "A survey on the internet of things security," in *Computational Intelligence and Security (CIS), 2013 9th International Conference on*. IEEE, 2013, pp. 663–667.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[8] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," *Sony Corporation*, pp. 7–10, 2008.

[9] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: State of the art," in *Robots and Sensor Clouds*. Springer, 2016, pp. 55–75.

[10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. IEEE, 2012, pp. 257–260.

[11] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*. IEEE, 2012, pp. 1282–1285.

[12] Y. R. Shi and T. Hou, "Internet of things key technologies and architectures research in information processing," in *Applied Mechanics and Materials*, vol. 347. Trans Tech Publ, 2013, pp. 2511–2515.

[13] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 4, pp. 2347–2376, 2015.

[14] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[15] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[16] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[17] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application." *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, 2011.

[18] M. Yun and B. Yuxin, "Research on the architecture and key technology of internet of things (iot) applied on smart grid," in *Advances in Energy Engineering (ICAEE), 2010 International Conference on*. IEEE, 2010, pp. 69–72.

[19] H.-E. Lin, R. Zito, and M. Taylor, "A review of travel-time prediction in transport and logistics," in *Proceedings of the Eastern Asia Society for transportation studies*, vol. 5, 2005, pp. 1433–1448.

[20] L. Coetzee and J. Eksteen, "The internet of things-promise for the future? an introduction," in *IST-Africa Conference Proceedings, 2011*. IEEE, 2011, pp. 1–9.

[21] M. L. Das, "Privacy and security challenges in internet of things," in *Distributed Computing and Internet Technology*. Springer, 2015, pp. 33–48.

[22] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for iot security," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*. IEEE, 2014, pp. 183–188.

[23] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things□a survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[24] B. Yan and G. Huang, "Supply chain information transmission based on rfid and internet of things," in *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on*, vol. 4. IEEE, 2009, pp. 166–169.

[25] C. Sarkar, S. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying iot applications," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 2014, pp. 508–513.

[26] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, 2013.

[27] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[28] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[29] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks." in *NDSS*, 2002.

[30] M. L. Das, "Two-factor user authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 3, pp. 1086–1090, 2009.

[31] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *Etri Journal*, vol. 32, no. 5, pp. 704–712, 2010.

[32] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[33] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the internet of things: selected challenges," *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, pp. 31–34, 2009.

[34] H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in *Coping with Global Environmental Change, Disasters and Security*. Springer, 2011, pp. 61–106.

[35] G. S. Matharu, P. Upadhyay, and L. Chaudhary, "The internet of things: Challenges & security issues," in *Emerging Technologies (ICET), 2014 International Conference on*. IEEE, 2014, pp. 54–59.

[36] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.

[37] T. Landstra, M. Zawodniok, and S. Jagannathan, "Energy-efficient hybrid key management protocol for wireless sensor networks," in *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*. IEEE, 2007, pp. 1009–1016.

[38] C. Qingling, Z. Yiju, and W. Yonghua, "A minimalist mutual authentication protocol for rfid system & ban logic analysis," in *Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on*, vol. 2. IEEE, 2008, pp. 449–453.

[39] S. Kalra and S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *Journal of Information Security and Applications*, vol. 20, pp. 37–46, 2015.

[40] W. Drira, E. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for wban," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 78–83.

[41] C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor networks," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 1. IEEE, 2007, pp. 438–442.

[42] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 26, no. 2, pp. 181–201, 2014.

[43] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee, and H. Lee, "A strong authentication scheme with user privacy for wireless sensor networks," *ETRI journal*, vol. 35, no. 5, pp. 889–899, 2013.

[44] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10 081–10 106, 2014.

[45] C.-H. Huang, H.-H. Wu, Y.-J. Huang, W.-C. Lin, C.-L. Pan, S.-I. Chu, and P.-Y. Chen, "Lightweight authentication scheme for wireless sensor networks," in *2012 IEEE Global High Tech Congress on Electronics*, 2012.

[46] N. Ye, Y. Zhu, R.-C. Wang, R. Malekian, and L. Qiao-min, "An efficient authentication and access control scheme for perception layer of internet of things," *Applied Mathematics & Information Sciences*, vol. 8, no. 4, p. 1617, 2014.

[47] O. Delgado-Mohatar, A. Fúster-Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 727–735, 2011.

[48] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks," in *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*. Citeseer, 2002, p. 7.

[49] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[50] A. K. Das, V. Odelu, and A. Goswami, "A robust and effective smart-card-based remote user authentication mechanism using hash function," *The Scientific World Journal*, vol. 2014, 2014.

[51] X. Zhou and Y. Xiong, "An efficient and lightweight user authentication scheme for wireless sensor networks," in *Information Computing and Applications*. Springer, 2011, pp. 266–273.

[52] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[53] M. A. Crossman and H. Liu, "Study of authentication with iot testbed," in *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 1–7.

[54] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*. ACM, 2007, pp. 9–14.

[55] O. Cheikhrouhou, A. Koubaa, M. Boujelben, and M. Abid, "A lightweight user authentication scheme for wireless sensor networks," in *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on*. IEEE, 2010, pp. 1–7.

[56] D. He, "Robust biometric-based user authentication scheme for wireless sensor networks." *IACR Cryptology ePrint Archive*, vol. 2012, p. 203, 2012.

[57] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for internet of things," in *Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on*. IEEE, 2011, pp. 563–566.

[58] S. I. Ahamed, F. Rahman, and E. Hoque, "Erap: Ecc based rfid authentication protocol," in *Future Trends of Distributed Computing Systems, 2008. FTDCS'08. 12th IEEE International Workshop on*. IEEE, 2008, pp. 219–225.

[59] K. Chatterjee, A. De, and D. Gupta, "A secure and efficient authentication protocol in wireless sensor network," *Wireless Personal Communications*, vol. 81, no. 1, pp. 17–37, 2015.

[60] R. Fan, D.-j. He, X.-z. Pan *et al.*, "An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks," *Journal of Zhejiang University SCIENCE C*, vol. 12, no. 7, pp. 550–560, 2011.

[61] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58–67, 2011.

[62] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee, and H. Lee, "A strong authentication scheme with user privacy for wireless sensor networks," *ETRI journal*, vol. 35, no. 5, pp. 889–899, 2013.

[63] D. Kyriazis and T. Varvarigou, "Smart, autonomous and reliable internet of things," *Procedia Computer Science*, vol. 21, pp. 442–448, 2013.

[64] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*. IEEE, 2013, pp. 88–93.

[65] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (iecac) scheme for internet of things," in *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*. IEEE, 2012, pp. 187–191.

[66] A. Mnif, O. Cheikhrouhou, and M. B. Jemaa, "An id-based user authentication scheme for wireless sensor networks using ecc," in *Microelectronics (ICM), 2011 International Conference on*. IEEE, 2011, pp. 1–9.

[67] S. C. Mukhopadhyay and N. Suryadevara, *Internet of Things: Challenges and Opportunities*. Springer, 2014.

[68] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[69] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014.

[70] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272–276, 2010.

[71] Y. M. Yussoff, H. Hashim, and M. D. Baba, "Identity-based trusted authentication in wireless sensor network," *arXiv preprint arXiv:1207.6185*, 2012.